HIGH COURT OF MADHYA PRADESH
PRINCIPAL BENCH JABALPUR

<u>Subject: The matter regarding the infrastructure Gap Analysis report regarding IT network infrastructure.</u>

Under the subject cited above, it is to submit that the gap analysis survey has been conducted jointly by the CISCO team and High Court technical team in order to carry out the security of the network and to fill the I.T. gaps in the existing infrastructure.

The following are the gaps pertaining to security and Network infrastructure gaps as per details given below:-

1) Network is not designed properly or has grown in a inorganic manner
2) Network is extended using cascading.
3) Most of the other buildings from camps are connected through court rooms.
4) Single point of failure is the major challenge(links and devices)
5) Layer 2 loops is another challenge
6) Non scalable Network hub rooms
7) Lack of Active-Active architecture on wired and wireless
8) Lack of Wireless LAN Security / Weak Security
9) Cabling need to be upgraded to support higher speed and POE standards
10) Wireless network to be redesigned using proper survey
11) Absence of a network monitoring system
12) No visibility of network, clients connected and applications running over the network.

25/01/2024

Back

13) No network troubleshooting tool
14) No Underlay last mile visibility across MPSL Service providers
15) Multiple management touch points or manual approach

Security Infrastructure Gaps

1) No Device Login AAA
2) Only authentication is enabled for wireless users which is currently shared with anybody
3) No user access and control AKA network admission and control for wired and wireless
   a. No Users authentication
   b. No Device authentication
   c. No Deviceprofiling
   d. No Device posturing with reference to MP-HC policies
   e. No Multi Factor authentication
   f. No segmentation
4) Lack of DNS security solution for secure internet access for Wired and wireless uses.
5) Absence of Enterprise Class Firewall @ MP-HC Court room building.
6) No Secure infrastructure to secure the High court website in SDC.
7) Absence of LAN Analytics for anomalous behavior.
8) No solution to identify the malicious behavior within encrypted flows

25/01/2024

Back

Also, it is further submitted that the following immediate action is required as per details given below:-

1. To Integrate ISE server with advocate registration database for providing authentication and logging.
2. Properly segment the wireless SSID and VLAN for advocates and carry the VLAN directly to the internet gateway.
3. Maintain separate VLAN for court employees and staff.
4. Deploy separate VLAN for CCTV, Wi-Fi, management of devices etc.
5. ***Protect the High Court website by introducing a WAF (WEB APPLICATION FIRE WALL) and Load Balancer***.
6. Place an enterprise grade pair of firewall in front of the application servers. This is most critical as it is a public facing website.
7. Integrate access switches with ISE for AAA (device management) and user authentication. Augment the licenses needed by purchasing additional licenses.
8. Looking at emerging threat vectors it is important to deploy DNS Security for all users which can provide first level of defence against any DNS attack arising.
9. Deploy XDR platform for all users to protect against any probable security breach.

25/10/2024

Back

HIGH COURT OF MADHYA PRADESH
PRINCIPAL BENCH JABALPUR

Sub:- Regd. the infrastructure Gap Analysis report regd. IT network infrastructure.

The detailed report is placed as per **"Flag-A"** for kind perusal, please.

Hence, the matter to fulfill the infrastructure gap of network infrastructure and to enhance the security from the viruses, worms, outside and inside network attacks and to remove network glitches may be placed before the I.T. and e-Courts Committee of the High Court for consideration and recommendations.

Therefore, may if approved: -

1. Permit to place the matter to fulfill the infrastructure gap of network infrastructure and to enhance the security from the viruses, worms, outside and inside network attacks and to remove network glitches, before the I.T. and e-Courts Committee of the High Court for consideration and recommendations.

25/01/24

(F.H. QAZI)
SPSA(SA)

Hon'ble Ch., Committee for [illegible]

REGISTRAR GENERAL

7.1.2024

HON'BLE SHRI JUSTICE ROHIT ARYA
(CHAIRMAN, I.T. & E-COURTS COMMITTEE)

Back

Infrastructure Gap Analysis Report

Submitted to

Madhya Pradesh High Court

THE HIGH COURT OF MADHYA PRADESH

सत्यमेव जयते

Submitted by

Cisco Systems

Back

Table of Contents

Purpose of this report

Cisco has conducted Tech Day for Madhya Pradesh High Court team on Secure Networking, Collaboration and Security. As an action item of Tech Day – MP-HC requested Cisco to do a Gap Analysis of network and security infrastructure and come up with findings in a report. This report provides an overview of the gaps and also suggests the remediation to overcome the gaps and strengthen the overall Network and Securty design and posture.

Infrastructure Gaps

Network infrastructure Gaps

1) Network is not designed properly or has grown in a inorganic manner
2) Network is extended using cascading
3) Most of the other buildings from campus are connected through court rooms.
4) Single point of failure is the major challenge(links and devices)
5) Layer 2 loops is another challenge
6) Non scalable Network hub rooms
7) Lack of Active-Active architecture on wired and wireless.
8) Lack of Wireless LAN Security / Weak Security
9) Cabling need to be upgraded to support higher speed and POE standards
10) Wireless network to be redesigned using proper survey
11) Absence of a network monitoring system
12) No visibility of network, clients connected and applications running over the network.
13) No network troubleshooting tool
14) No Underlay last mile visibility across MPLS Service providers
15) Multiple management touch points or manual approach

Security Infrastructure Gaps

1) No Device login AAA
2) Only authentication is enabled for wireless users which is currently shared with anybody.
3) No user access and control AKA network admission and control for wired and wireless
    a. No User authentication
    b. No Device authentication
    c. No device profiling
    d. No device posturing with reference to MP-HC policies.
    e. No Multi Factor authentication
    f. No segmentation
4) Lack of DNS security solution for secure Internet access for Wired and wireless users.
5) Absence of Enterprise Class Firewall @ MP-HC Court room building.
6) No Secure infrastructure to secure the High court website in SDC.
7) Absence of LAN Analytics for anomalous behaviour
8) No Solution to identify the malicious behaviour within encrypted flows.

Back

Physical infrastructure Gaps

(Need to be filled by partner)

UPS
Power
Cabling
Man power

Architecture Recommendations

Secure Network infrastructure

1) Switches should support SD-LAN or Legacy switching architecture (2 or 3 tier)
    a. Will elaborate the benefits of SD-LAN later
2) Access Data Switches should support 1G host ports with 4x10/25G uplinks on Fiber
3) Access POE switches should support Multi-Gig (1/2.5/5/10G) with 4x10/25G uplinks on Fiber
4) Access POE switches should support advance POE/POE+/UPOE standards and features to support HD Cameras, WIFI6/7 access points and various POE enabled Devices.

5) Wireless AP need to be upgraded to latest models supporting variety of radio's (2.4/5/6 Ghz) and dedicated radio's for scanning along with higher speed and advance technologies.

    For Indoor clients –We should have an access point which can cater to higher user density and deliver higher throughputs based on latest and futuristic standards.

    a. Hexa-Radio Architecture
        i. 2.4 GHz Serving Radio (Slot 0): 4x4:4SS
        ii. 5 GHz Serving Radio (Slot 1 + Slot 2): 8x8:8SS
        iii. Dual 5 GHz Serving Radio (Slot 1 or Slot 2*) 4x4:4SS
        iv. 6 GHz Serving Radio (Slot 3): 4x4:4SS
        v. Dedicated AI/ML-Driven Scanning Radio: Dedicated radio for aWIPS, interference detection and mitigation
        vi. 2.4 GHz IoT Radio
    b. Dual PoE for Power Redundancy
        i. 2 x 5 Multigigabit (mGig) PoE Ports
        ii. 802.3 Link Aggregation > up to 10 Gbps uplink
    c. Internet of Things Capabilities
        i. Built-In Environmental Sensors
        ii. Application Hosting Technology
        iii. USB port with 9W power output

    For outdoor clients – We should have access point based on latest and futuristic standards.

    Wireless WLC should be in pair hosted in Jabalpur DC (shared services) to support Client and AP SSO/HA and another WLC (single or pair) in SDC to support N+1 HA architecture.

Back

6) Access (Data / POE) switches should support 802.1AE MACSEC functionality to enable secure transport on Layer 2 between access to distribution.
    a. To safeguard from MITM attacks.
7) Access switches uplinks should be in an Ether-Channel (LACP) connected to dual distribution switches within each building.
8) Each court room should have 48 port MGIG switches to support existing and future port requirements.
9) Outside each court we should have scalable network hub room supporting multiple access switches in a rack (Multiple access switches part of single stack)

10) Each Building will have minimum one pair of distribution switch.
11) Distribution switches should support 10/25G downlink ports (connecting to access switches) and 40/100G uplink ports (connecting to core switches).
    a. Distribution switches should be in SVL/VSS to support A-A function to access switches on downlinks and A-A function to core switches on uplinks
    b. Distribution switches should have Layer 3 GW for each VLAN
    c. Separate VRF for critical subnets / segments like Exam Center/ Court rooms etc.
12) Layer 3 routing (OSPF/BGP) between Distribution and Core Switches.

13) Core switches should be in DC Network room supporting A-A function using SVL/VSS.
14) Core switches should be connected to Firewall pairs using 10/25/40G ports.
    a. Two separate firewall pairs – 1 for securing intranet apps and 2nd for perimeter/internet
15) Above Perimeter Firewall pair there should be pair of routers supporting Internet and SD-WAN routing to filter the IN and OUT Traffic.

16) Access, Distribution and Core switches should support NETFLOW to gain visibility across all the layers
    a. Behaviour anomaly in the campus LAN
    b. Malicious traffic inside encrypted channels.

Network Management System

Automation

c. Network device configurations using templates
d. Network device monitoring
e. Network device configuration and firmware compliance
f. POE analytics and WIFI 6 readiness dashboard

Assurance / Analytics

a. Client, Network device (wired and wireless) and Applications for last 30 days
b. Trending information comparisons with reference to baseline changes.
c. Client End point information using Multi Factor Classifications (EP analytics)
d. Each End point will get trust score from ISE and integration with various security solutions and research engines like TALOS.
e. Integration between NMS and NAC so that End point can be contained / isolated from single dashboard.
f. Client search using hostname (Integration with ISE/NAC is required)
g. Group base policy analytics (Group = SGT = ISE is must) to define the security policies between two end points groups (Defined in MS-SQL)
h. Wireless Intrusion and prevention system to identify rogue access points, rogue clients over the floor map and remediation/isolation.
i. Advance wireless enhancements like 3D Maps to identify coverage issues, AI-RRM
j. AI and ML is used to provide steps to fix the issues from issue dashboard.

k. Security vulnerabilities compliance provides visibility across the network devices/firmware and its automatically updates on a frequent basis. With this information, Admin can schedule the downtime and roll out the upgrade plan

Design Recommendations

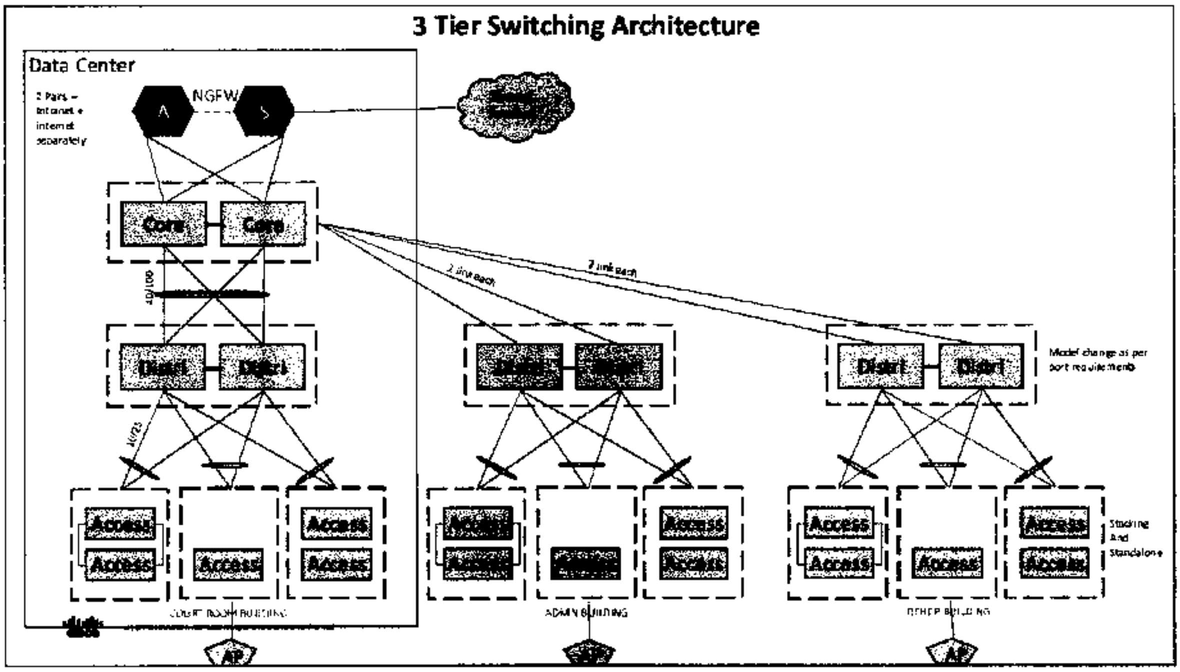
Switching Design

There can be two types of switching design –

1) Standard legacy switching and wireless design where switches are connected in 2 or 3 tier architecture and access points are connected to POE access switches and WLC is connected to Firewall in shared services ~~zone and both are connected in either central or flex-connect mode.~~

2) SDN / SDA – Fabric base design made of 2 or 3 tier switching architecture including fabric enabled wireless design so that single identity base policy can be used for user while on-boarding on wired and wireless network. Policy can be defined on single dashboard with multiple other benefits.

Design 1 - Standard legacy Switching Design

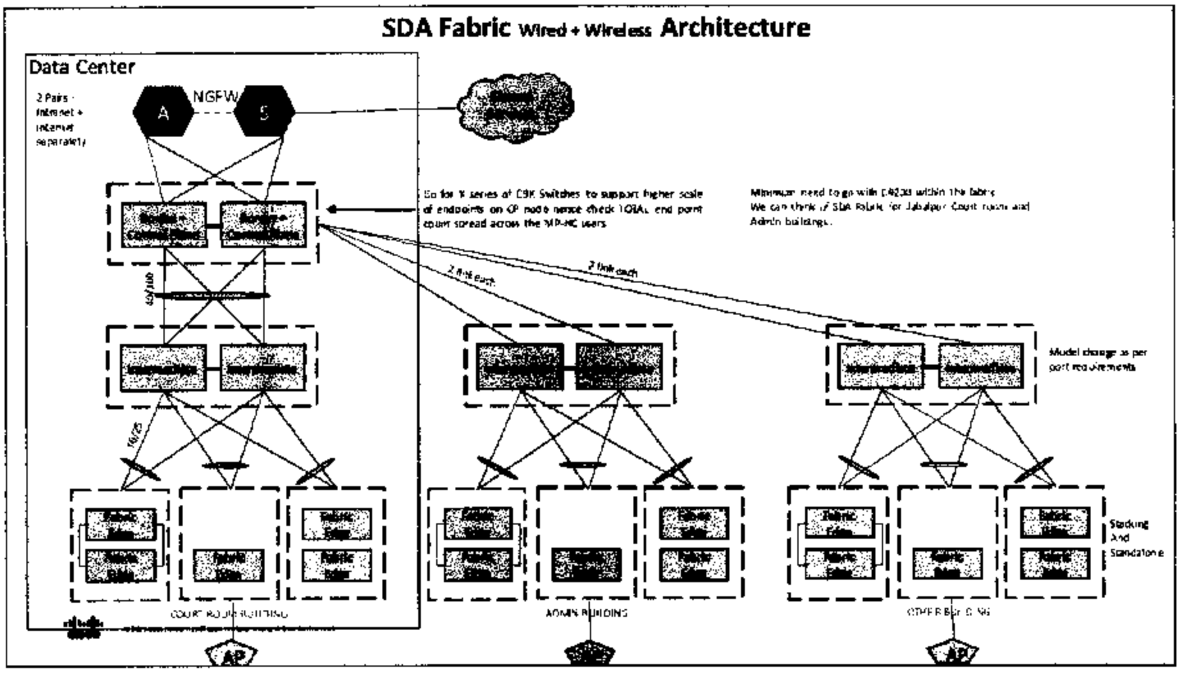


Benefits of Design 1

1. Access switches can work in standalone or stacking mode; stacking provide single configuration file for configuration management and uplinks from different switches to provide resiliency.
2. Access switches sees one logical distribution switch in spite of two physical switches with uplinks in in Active-Active manner. Logical switching system built using SVL/VSS technology.

3. No chances of Layer 2 loops however if it happens then it will impact that building only as L3 is on that building's distribution switch and above that pure play layer 3 routing.
4. Necessary routing table will be available in distribution switches – Default route to reach internet and specific routes to reach other Servers hosted in DC and SDC. This can be possible by doing route summarization on Core switches.
5. Access to Distribution on multiple 10/25G links and Distribution to Core on multiple 40/100G links and 10G towards Firewall pairs. (Ideally should have separate pairs for internet and Intranet)
6. Firewalls will be in Active Standby and all traffic going out and coming in from Internet, SDC and from SD-WAN sites will get filtered using perimeter NGFW.

Design 2 - SDA – Fabric base design with fabric enabled wireless



SDA Fabric Wired + Wireless Architecture

Go for X series of C9K Switches to support higher scale of endpoints on CP node hence check TOTAL end point count spread across the MP-HC users

Minimum need to go with C9200 within the fabric
We can think of SDA Fabric for Jabalpur Court room and Admin buildings.

Benefits of design 2

1) Simplifies network operations with a standard, error-free underlay network using LAN automation.
2) Only 3 protocols to run the fabric – ISIS to run underlay, LISP for running overlay and VXLAN to data forwarding. This approach reduce lots of configuration mistakes, protocols overheads etc.
3) 3 planes in the fabric – Control plane is LISP, Data plane is VXLAN and Policy plane is ISE
   a. LISP to tell where is your destination – A new approach in digital journey
      i. LISP tracks end point movement and maintain/update the database.
   b. VXLAN to support massive scale of segments as well as use to encap/decap traffic within the fabric from source to destination.
   c. ISE to support onboarding of users and devices, profiling, posturing and segment them using identity base security policy configurations called secure group tags
4) No Layer 2 loops within the fabric as ISIS protocol is used between access/edge to Core/Border Node for routed access.
5) VLAN boundary or layer 2 handoff is on Fabric edges.
6) VLAN to VXLAN Network identifiers mapping for Layer 2 or Layer 3 communications.

7) Fabric provides support for end hosts that require Layer-2 flooding; for example, building management systems, audio-visual equipment, etc. (if required)

8) Anycast GW support for seamless Layer 3 mobility across the overlay fabric for endpoints.
    - a. If user moves over wireless network then also no need to GARP.
    - b. If user moves from one building to another building, he will get same policy.
        - i. Both scenario –
            - 1. If user gets same IP then no need to GARP.
            - 2. If user gets different IP then also they will get same policy using identity.

9) SD-Access, through Cisco DNA Center, creates virtual overlays over the underlying physical infrastructure and segments the network without regard to its topology.

10) SD-Access also segments at a micro level by enforcing identity base group-based policies through the network infrastructure. The resulting granular segmentation controls traffic flows without using complex firewalls and Access Control Lists (ACLs), which can be difficult and costly to maintain.

11) Zero Trust Network infrastructure –
    - a. Identity base SGACL can be defined on DNA-C – Single unified converged policy for Wired and wireless networks.
        - i. Simple to define using tags (No relation with IP addresses)
        - ii. If someone like Auditor/Contractor is finish the work and move on and you need to remove the policies/configuration then its very easy and agile to do the same.

12) SD-Access fabric offers two options for integrating wireless access:-
    - SD-Access Wireless using a VXLAN distributed data plane and a centralized control plane provides a consistent fabric experience and policy simplification for wired and wireless access.
        - o WLC is out of band and that job is given to switches - distributed data plane with wireless mobility
        - o WLC talks to LISP Control plane to help track end point mobility
    - Over the top involves running a traditional Cisco Unified Wireless Network architecture with Control and Provisioning of Wireless Access Points (CAPWAPs) on top of a fabric wired network. This is a possible migration step to full SD-Access wireless implementation.

13) IT and OT Convergence using VRF base logical segmentation over the fabric.

Security Design

Secure User Onboarding and Access

1) If user access Network Devices then there should be TACACS software to log following –
   a. A - Who has logged into the device?
   b. A – What level of Authorization this user has?
   c. A - What changes user has done on this device?

2) Before user on-board and gain access to the network ideally solution should check following –
   a. Use agent based port network admission control (NAC solution) base on 801.X protocol to verify user Authentication thru AD / SQL server.
      i. AD is recommended as it will be useful for ISE and Umbrella as well
   b. On granular level the advance NAC solution System should have ability to verify the user authentication part before getting IP address from DHCP using Layer 2 EAP/8021.X/RADIUS protocols between user, network device and radius server.
   c. NAC solution should provide visibility of connected user devices like Laptop, Mobile devices, Printers, Scanners and Network and security devices from the overall infrastructure under profiling.
   d. NAC solution should do posture check of endpoint by verifying the status of AV version, APT version, MS SCCM Patch version and specific application which need to be available on the user end point as per the corporate policy to identify that it's an corporate device.
   e. NAC solution should provide basic VLAN and Downloadable Access-list as well as identity base logical segmentation on wired and wireless network.
   f. Use Multi Factor authentication to provide additional security to confirm the legitimate user thru passcode verification or approval request on mobile devices which are running MFA application.

Note:- CISCO ISE can provide you both device administration, Port base NAC functionality and integration with DUO for Multi Factor authentication.

Additional Cisco ISE integrations –

1) Cisco ISE has native PXGRID (policy exchange) REST API to exchange data with others
2) Cisco ISE can be integrated with DNA-C (NMS) to share the identity information –
   a. Client search can be done using User name.
   b. Identity to Identity or unknown communication is logged under policy analytics.
   c. Trust analytics per user to understand the trust score

3) Cisco ISE can be integrated with Cisco SNA to understand user behaviour and take action – Cisco SNA solution can identify abnormal behaviour of users on the network and to identify malicious communications inside encrypted channels.
4) Cisco ISE can be integrated with Vulnerability detection OEMs so that on-boarded user can be isolated once it is detected vulnerable using Rapid threat containment solution.

Segmentation of Users, Endpoints and with Exam Centre -

All Security guidelines are highlighting that logical or physical segmentation should be available across the Campus and Data Centre network to avoid bi-lateral movements or communications of malicious traffic.

There are multiple ways thru which we can achieve segmentations –

Macro and Micro Segmentations –

Macro Segmentation -

1) LAYER 2 – VLAN Based (Source Base)
2) Layer 3 – VRF instance to isolate segment (Source base) – Virtual routing and forwarding

Micro Segmentation –

1) PVLAN – Private VLAN (Complex to configure and manage)
2) Secure Group Tag – Identity base (Simple to manage at huge scale)

Due to in absence of Active Directory, MP-HC need to define the User types in MS-SQL and in Cisco ISE locally.

However to define the identity base policy - MP-HC must know which applications are accessible by which users.

Few examples of logical identity base segmentations – Judges, Judges steno, assistants, registrar, assistants, IT teams, Advocates over wireless, Server to subnet mapped SGT.

1) Judges and Judges steno and assistant from court room are part of same VLAN and VRF however can't talk to each other unless it's required to run the court room. Otherwise, each identity can access relevant allowed applications only.

2) Exam Centre can be completely isolated using dedicated VRF and completely isolated with Micro Segmentation using SGT base identity however USB ports can be disabled on those endpoints.

Identity classification can be done at Authentication level and Identity base policy enforcement can be done at multiple levels like –

1) East to West traffic filter on switching level – Egress switch ports (Access / Core)

2) South to North traffic filter on Core Switch or best to do it on Firewalls.

Secured networking with LAN Analytics

All switches from Access to Core and from DC side as well should support NETFLOW (Capability to export L2 to L7 information using Flows). Need to enable NETFLOW feature on switches and router so that we can export it to Behaviour and Anomaly engine called SNA (Secure Network Analytics) which can run Machine learning and do behaviour modelling on the collected data and come up with following visibility against Campus endpoints which do active data forwarding –

1) Abnormal behaviour over the Campus LAN
    a. Data hording
    b. Data ex-filtering
    c. Target/Compromised endpoints
    d. Non legitimate communications/ flows
    e. And many others

2) Malicious communications under the encrypted channel (HTTPS)

Secured internet browsing for Users and Advocates connected on HC LAN/WLAN

Step 1 -

Today Users are categorized into Court room, Registrar offices, IT team and others called Type 1 – Known while Advocates are using like free internet with minimal security and restrictions using Sonicwall Firewall which we will called Type 2.

Cisco Umbrella DNS security is the First level of Defence for any type of internet communication, need to configure specific Cisco Umbrella DNS servers IP addresses into the DNS servers setting of Type 1 users endpoint so that they will be protected when they will work from office campus LAN or when they will work remotely like work from home.

Authentication can be done using Organizations AD thru Umbrella and right policy can be placed against each user.

For Type 2 users – Who are advocates and only access thru wireless LAN. For them we need to configure Umbrella DNS entries and DNS redirection configuration on Cisco wireless controllers.

Authentication can be done using Organizations SQL server using ISE through Umbrella and right policy can be placed against each Type 2 user (SSID - Advocate).

Step 2 –

Post covid, IT team has ask to deliver single security policy for internet and intranet access while working from office or work from home so that there will be less overhead for IT teams with reference to configuration management and monitoring.

Answer is Cisco Secure Access based on Identity AKA Secure group tag.

This tag will be applied to wired or wireless users over campus LAN and get filtered on on-prem Firewall for policy management and same tag will be used in cloud security solution called Cisco Secure Access for work from home users. This brings simplicity, agility in overall management with no complexity.

Securing the High Court website hosted in SDC

Anyone in the world can access High court website as its publically available however the correct security is not in place hence following design need to be factored so that website setup can be protected from hackers.

Today all communications is secured using HTTPS (TLS 1.2 and above) however we never decrypt the packet and check whats inside due to privacy however we can re-design the setup to provide the best secure design.

1) Need to take clean pipe service from Internet service providers so that they can filter the DDOS attacks and forward clean internet traffic to MP-HC web site.
2) Need devices to decrypt the TLS/HTTPS traffic and hand it over to NGFW.
3) **NGFW modules will filter the traffic over ports and signatures and return back to encryption device if you want to keep end to end encryption till webserver or firewall will forward clear text traffic to web servers directly.**
4) We need to factor Server load balancers before Web servers so that tomorrow if the web servers grows from one to two or many we can load balance the incoming sessions on each servers and make the best use of server infrastructure. A Web Application Firewall will provide security against application layer attacks. The load balancer / Application delivery controller can provide WAF functionality on the same box.
5) Ideally we should have one more firewall layer between Web and APP or DB however its completely depend on organization requirement.

Network and Security revamp in JBP DC

Currently Non Enterprise category firewall is installed in Jabalapur DC and used to protect all Internet bound traffic from MP-HC offices spread across Madhya Pradesh.

Recommendation is to use two NGFW pairs – 1 for intranet applications and 2nd for internet (perimeter) with identity base functionality so that tags will get classified on authentication while onboarding over the network thru wired or wireless and get filtered on Firewall with reference to access policies like Ports, URL-F, Content etc.

Underlay last mile visibility

Currently Cisco provides Internet path and communication visibility using Thousand eyes solution but the challenge is there is no visibility on MPLS as last mile where MPLS SP has not allowed ICMP etc.

Today MP-HC setup is spread across MP using BSNL as MPLS provider however with zero visibility.

This challenge is there for many enterprise customer hence Cisco has done a recent acquisition of Accedian which can provide the MPLS last mile visibility hop by hop using proper dashboarding and reporting, this solution use different port and protocols apart from ICMP.

Action Items

Immediate

1. Integrate ISE with advocate registration database for providing authentication and logging.
2. Properly segment the wireless SSID and VLAN for advocates and carry the vlan directly to the internet gateway.
3. Maintain separate vlans for court employees and staff
4. Deploy separate vlans for CCTV, Wifi, management of devices etc.
5. Protect the High Court website by introducing a WAF and Load Balancer.
6. Place an enterprise grade pair of firewall in front of the application servers. This is most critical as it is a public facing website.
7. Integrate access switches with ISE for AAA (device management) and user authentication. Augment the licenses needed by purchasing additional licenses.
8. Looking at emerging threat vectors it is important to deploy DNS Security for all users which can provide first level of defence against any DNS attack arising
9. Deploy XDR platform for all users to protect against any probable security breach

Near Term

1. Revamp entire cabling and have redundancy and resiliency at each level.
2. Proper rack dressing and racks need to be locked for physical security.
3. Based on long term plan, correct the switching design by adopting either design 1 or 2. Any necessary upgrade of licenses and / or devices should be procured.
4. The active and passive design have to go hand in hand.
5. Procure new Access Points for Court rooms and re deploy the ones deployed there to other locations.
6. After the security controls are in place, consider allowing case management system over wifi.
7. Deploy SoC for security operations once all security sensors are in place