ACCESS MANAGEMENT

SMT GROUP

ACCESS MANAGEMENT

IN THE WORLD OF CYBERSECURITY, **THREE ESSENTIAL TECHNOLOGIES** ARE USED TO PROTECT ACCESS TO COMPANY RESOURCES:

1. **IAM** (IDENTITY AND ACCESS MANAGEMENT)
2. **PAM** (PRIVILEGED ACCESS MANAGEMENT)
3. **ZTNA** (ZERO TRUST NETWORK ACCESS)

IDENTITY AND ACCESS MANAGEMENT

IAM IS A CYBERSECURITY TECHNOLOGY DESIGNED TO MANAGE AND CONTROL USER ACCESS TO A COMPANY'S SYSTEMS AND RESOURCES. **ITS PURPOSE IS TO ENSURE THAT ONLY AUTHORIZED PEOPLE CAN ACCESS THE RIGHT RESOURCES UNDER THE APPROPRIATE CONDITIONS**, MANAGING BOTH IDENTITIES AND ACCESS PERMISSIONS

FEATURES

IDENTITY MANAGEMENT: PROVIDES A CENTRALIZED SYSTEM FOR CREATING, MODIFYING, AND DELETING USER ACCOUNTS

USER AUTHENTICATION: VERIFIES USER IDENTITY USING PASSWORDS, MULTI-FACTOR AUTHENTICATION (MFA), AND OTHER METHODS

AUTHORIZATION AND ACCESS CONTROL: CONTROLS WHICH USERS HAVE ACCESS TO WHICH RESOURCES AND UNDER WHAT CONDITIONS, USING ROLE-BASED ACCESS CONTROL (RBAC) POLICIES

COMPLIANCE: FACILITATES COMPLIANCE WITH PRIVACY AND SECURITY REGULATIONS

WHAT IAM DOES

IDENTITY MANAGEMENT: THE PROCESS OF CREATING, STORING AND MANAGING IDENTITY INFORMATION. IDENTITY PROVIDERS (IDP) ARE SOFTWARE SOLUTIONS THAT ARE USED TO TRACK AND MANAGE USER IDENTITIES, AS WELL AS THE PERMISSIONS AND ACCESS LEVELS ASSOCIATED WITH THOSE IDENTITES

IDENTITY FEDERATION: ALLOW USERS WHO ALREADY HAVE PASSWORDS ELSEWHERE (FOR EXAMPLE, IN YOUR ENTERPRISE NETWORK OR WITH AN INTERNET OR SOCIAL IDENTITY PROVIDER) TO ACCESS YOUR SYSTEM

PROVISIONING AND DEPROVISIONING OF USERS: CREATE AND MANAGE USER ACCOUNTS, INCLUDING SPECIFYING WHICH USERS CAN ACCESS WHICH RESOURCES AND ASSIGNING PERMISSIONS AND ACCESS LEVELS

WHAT IAM DOES

AUTHENTICATION OF USERS: CONFIRM THAT A USER, MACHINE OR SOFTWARE COMPONENT IS WHO OR WHAT THEY CLAIM TO BE

AUTHORIZATION OF USERS: ENSURES A USER IS GRANTED THE EXACT LEVEL AND TYPE OF ACCESS TO A TOOL THEY ARE ENTITLED TO

ACCESS CONTROL: THE PROCESS OF DETERMINING WHO OR WHAT HAS ACCESS TO WHICH RESOURCES, THIS PROCESS INCLUDES DEFINING USER ROLES AND PERMISSIONS, AS WELL AS SETTING UP AUTHENTICATION AND AUTHORIZATION

IAM

01 SINGLE SIGN ON

02 PASSWORD MANAGEMENT

03 MULTI-FACTOR AUTHENTICATION

04 AUTHENTICATION & AUTHORIZATION

05 USER & IDENTITY MANAGEMENT

06 ACCESS MANAGEMENT

PAM (PRIVILEGED ACCESS MANAGEMENT)

PAM IS A SECURITY SOLUTION THAT **FOCUSES ON PROTECTING ACCOUNTS WITH PRIVILEGED ACCESS**, SUCH AS SYSTEM, DATABASE, OR CRITICAL APPLICATION ADMINISTRATORS

PRIVILEGED ACCESSES ALLOW USERS **TO MAKE SIGNIFICANT CHANGES TO SYSTEMS**, SO THEIR PROTECTION IS CRUCIAL TO AVOID SEVERE SECURITY BREACHES

FEATURES

PRIVILEGED ACCESS MANAGEMENT: CONTROLS ACCESS TO ACCOUNTS WITH ELEVATED PRIVILEGES, ENSURING ONLY AUTHORIZED USERS CAN TEMPORARILY ACCESS THESE ACCOUNTS

PRIVILEGE ESCALATION: ALLOWS USERS TO TEMPORARILY ESCALATE PRIVILEGES ONLY WHEN NECESSARY AND UNDER SUPERVISION, PREVENTING USERS FROM MAINTAINING ELEVATED PRIVILEGES CONTINUOUSLY

AUDITING AND MONITORING: TRACKS ALL ACTIVITIES PERFORMED BY USERS WITH ELEVATED PRIVILEGES, ENABLING AUDITS TO DETECT POTENTIAL ABUSES

DYNAMIC PASSWORDS: IN MANY CASES, PAM USES DYNAMICALLY GENERATED PASSWORDS FOR PRIVILEGED USERS, WHICH ARE CONSTANTLY RENEWED TO AVOID CREDENTIAL REUSE

REMOTE PRIVILEGED USER

AUDITOR

PRIVILEGED USER

MACHINE

SESSION MANAGEMENT

ASSET DISCOVERY

VAULT MANAGEMENT

DevOps

PASSWORD MANAGEMENT

IT ENVIRONMENT

APPS

CONTAINERS

APPS

DATABASE

OT ENVIRONMENT

OT MACHINES

OT WORKSTATIONS

ZTNA (ZERO TRUST NETWORK ACCESS)

ZTNA IS A SECURITY APPROACH THAT **ASSUMES NO PERSON OR DEVICE, INSIDE OR OUTSIDE THE NETWORK, IS TRUSTED BY DEFAULT**

INSTEAD OF ALLOWING FREE ACCESS WITHIN THE CORPORATE NETWORK, ZTNA REQUIRES CONTINUOUS VERIFICATION OF THE IDENTITY AND CONTEXT OF EACH ACCESS BEFORE ALLOWING ANY TYPE OF CONNECTION TO COMPANY RESOURCES

FEATURES

CONTINUOUS AUTHENTICATION: THE IDENTITY AND AUTHORIZATION OF USERS ARE VALIDATED CONTINUOUSLY, EVEN AFTER THE INITIAL AUTHENTICATION

MICRO-SEGMENTATION: DIVIDES THE NETWORK INTO SMALLER SEGMENTS, LIMITING ACCESS ONLY TO SPECIFIC APPLICATIONS AND DATA NECESSARY FOR THE TASK AT HAND, REDUCING THE ATTACK SURFACE

GRANULAR ACCESS: PROVIDES DETAILED CONTROL OVER WHICH APPLICATIONS, DEVICES, OR USERS CAN ACCESS SPECIFIC RESOURCES, BASED ON VERY SPECIFIC POLICIES

VISIBILITY AND CONTINUOUS MONITORING: MONITORS ALL INTERACTIONS AND ACTIVITIES OF USERS WITHIN THE NETWORK, PROVIDING FULL VISIBILITY OVER ACCESS

FEATURE	IAM	PAM	ZTNA
Main Focus	General identity and access management	Privileged access management	Zero Trust-based access management
Access Protection	Protects general access to systems and applications	Protects access to privileged accounts	Protects access to the network and resources based on identity and context
Auditing and Monitoring	Basic, focused on user access	Advanced, especially for privileged access	Advanced, continuous monitoring of access and behavior
Use Cases	Companies with many users and access to applications	Companies with critical systems and sensitive data	Distributed environments, remote work, and cloud
Privilege Control	Limited to general access	Full control over privileged access	Granular control of access, no trust in perimeter
Complexity	Moderate, easy to integrate	High, especially in complex environments	High, especially in traditional environments


IAM
PAM
ZTNA

IAM, PAM AND ZTNA

END-TO-END ACCESS PROTECTION: COVERS ALL USERS, DEVICES, AND ACCESS TYPES (REGULAR AND PRIVILEGED)

UNIFIED IDENTITY GOVERNANCE: CENTRALIZES USER LIFECYCLE, ONBOARDING, AND OFFBOARDING

ZERO TRUST ENFORCEMENT: CONTINUOUSLY VERIFIES USER IDENTITY AND DEVICE POSTURE BEFORE GRANTING ACCESS

IMPROVED OPERATIONAL EFFICIENCY: REDUCES MANUAL TASKS THROUGH AUTOMATION (SSO, PASSWORD ROTATION, SESSION MANAGEMENT)

COMPREHENSIVE VISIBILITY: PROVIDES FULL AUDIT TRAILS OF WHO ACCESSED WHAT, WHEN, AND HOW

IAM, PAM AND ZTNA

ENHANCED COMPLIANCE: SIMPLIFIES MEETING REGULATORY AND AUDIT REQUIREMENTS

STRONGER THREAT DEFENSE: PREVENTS CREDENTIAL THEFT, PRIVILEGE MISUSE, AND LATERAL MOVEMENT

SECURE REMOTE ACCESS: ZTNA REPLACES TRADITIONAL VPNS WITH IDENTITY-BASED, CONTEXT-AWARE ACCESS

CONSISTENT ACCESS POLICIES: ENSURES UNIFORM ENFORCEMENT ACROSS CLOUD, ON-PREM, AND HYBRID ENVIRONMENTS

BETTER USER EXPERIENCE: SEAMLESS LOGIN THROUGH IAM, SECURE PRIVILEGE ELEVATION VIA PAM, AND TRANSPARENT ACCESS WITH ZTNA

OTHER TELECOM TECHNOLOGIES

IN THE WORLD OF TELECOMMUNICATIONS, SMT SUPPORTED A SIGNALING FIREWALL AND TRAFFIC MANAGEMENT

THESE TECHNOLOGIES WORK TOGETHER TO SECURE AND OPTIMIZE NETWORK SIGNALING, ENSURING RELIABLE AND EFFICIENT COMMUNICATION BETWEEN ISP PROVIDER AND END USERS

SIGNALING FIREWALL

A SIGNALING FIREWALL IS A SECURITY LAYER FOR TELECOM NETWORKS THAT ANALYZES AND FILTERS SIGNALING MESSAGES, SUCH **AS SS7 AND DIAMETER**, TO PREVENT FRAUD, SPAM, AND OTHER THREATS

UNLIKE TRADITIONAL FIREWALLS THAT FILTER IP PACKETS, A SIGNALING FIREWALL INSPECTS MESSAGES FOR SPOOFING, CALL REROUTING, SMS HIJACKING, AND UNAUTHORIZED DATA LEAKS.

THESE SYSTEMS USE AI AND MACHINE LEARNING TO DETECT AND BLOCK MALICIOUS ACTIVITIES, PROTECT SUBSCRIBER DATA, AND ENSURE NETWORK INTEGRITY.

SIGNALING FIREWALL

KEY FUNCTIONS AND BENEFITS

THREAT DETECTION: IDENTIFIES AND BLOCKS MALICIOUS SIGNALING MESSAGES THAT COULD LEAD TO FRAUD, SUCH AS LOCATION SPOOFING, SMS HIJACKING, OR UNAUTHORIZED CALL REROUTING.

TRAFFIC VALIDATION: ENSURES THAT SIGNALING MESSAGES ORIGINATE FROM TRUSTED SOURCES AND VALIDATES THE CONTENT OF MESSAGES

COMPLIANCE ASSURANCE: HELPS TELECOMMUNICATION OPERATORS COMPLY WITH REGULATIONS LIKE GDPR BY SAFEGUARDING USER DATA

PROACTIVE PROTECTION: ACTS AS A PROACTIVE DEFENSE AGAINST REMOTE INTERCEPTION OF SMS, CALLS, AND SUBSCRIBER TRACKING

NETWORK INTEGRITY: PREVENTS SERVICE DISRUPTIONS AND PROTECTS THE OVERALL INTEGRITY AND SECURITY OF MOBILE NETWORKS

AI-POWERED SECURITY: LEVERAGES ARTIFICIAL INTELLIGENCE TO DETECT A WIDE RANGE OF THREATS, INCLUDING NEW AND EMERGING ATTACKS

TMO TRAFFIC MANAGEMENT SOLUTIONS

TMO (TRAFFIC MANAGEMENT OPTIMIZATION) FOCUSES ON IMPROVING NETWORK TRAFFIC FLOW AND OVERALL PERFORMANCE FOR TELECOM OR IT NETWORKS, ENSURING BETTER RESOURCE UTILIZATION, LOWER LATENCY, AND OPTIMIZED SERVICE DELIVERY

TMO PROVIDES SOLUTIONS AND SERVICES THAT ENHANCE TRAFFIC MANAGEMENT, INCLUDING:

TRAFFIC ANALYSIS & MONITORING: CONTINUOUS MONITORING OF NETWORK TRAFFIC TO DETECT CONGESTION POINTS OR INEFFICIENCIES

OPTIMIZATION ALGORITHMS: INTELLIGENT ALGORITHMS TO OPTIMIZE ROUTING, BANDWIDTH ALLOCATION, AND NETWORK RESOURCE UTILIZATION

POLICY-BASED TRAFFIC CONTROL: IMPLEMENTING RULES FOR PRIORITIZATION OF CRITICAL APPLICATIONS OR SERVICES

REPORTING & ANALYTICS: DETAILED INSIGHTS TO PLAN UPGRADES, EXPANSIONS, AND PREVENTIVE MAINTENANCE

TMO TRAFFIC MANAGEMENT SOLUTIONS

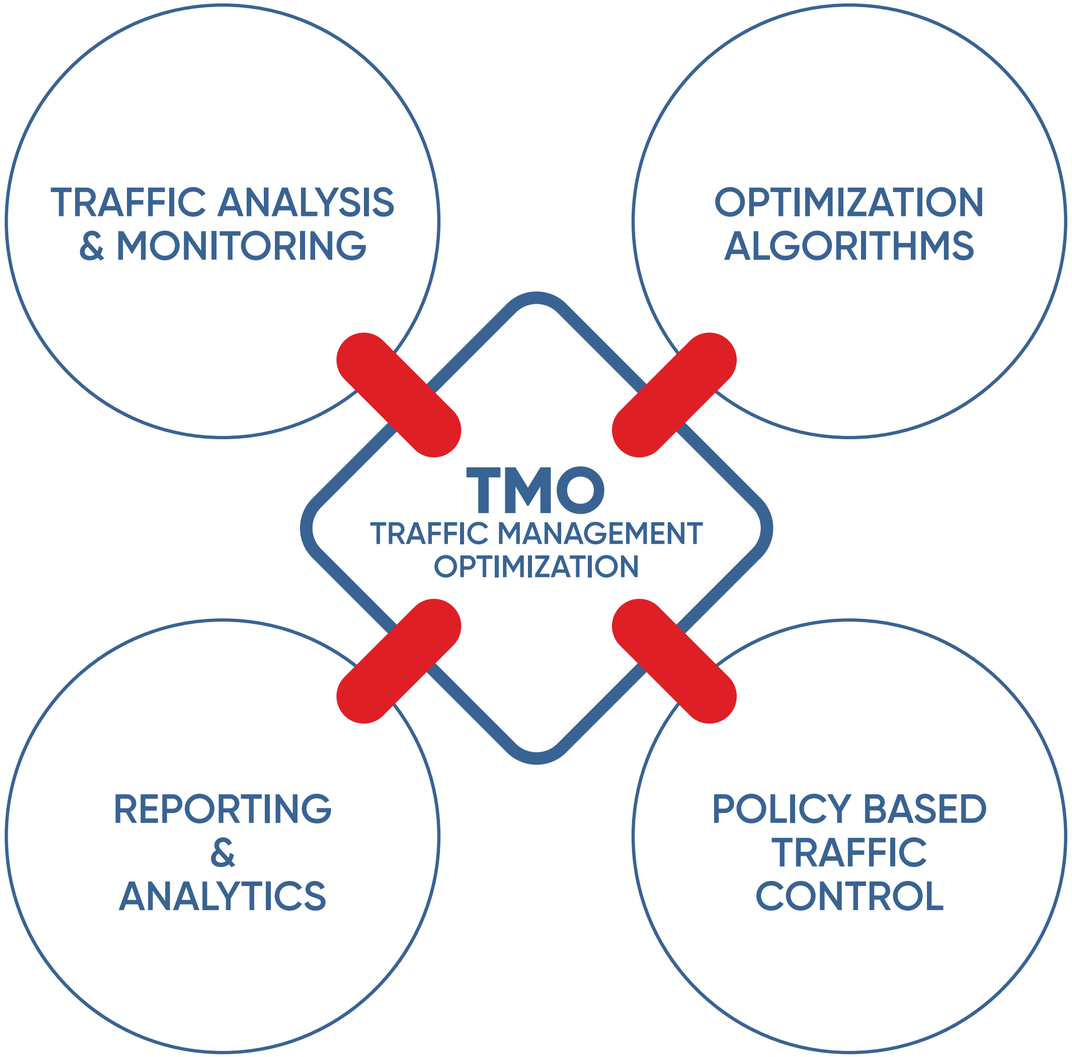
REDUCED NETWORK CONGESTION AND IMPROVED PERFORMANCE

ENHANCED QUALITY OF SERVICE (QOS) FOR CRITICAL APPLICATIONS

COST-EFFICIENT NETWORK MANAGEMENT BY OPTIMIZING EXISTING RESOURCES

PROACTIVE TROUBLESHOOTING AND CAPACITY PLANNING

TMO TRAFFIC MANAGEMENT SOLUTIONS



THANK YOU