Network Security Management Architecture

Effective network security requires a dedicated management system. This presentation explores the key tasks, integration approaches, and architecture of centralized, policy-based security management systems.

Core Management Tasks

Policy Management

Managing global security policy (GPB) and forming local security policies (LIB) for individual devices and information protection across the enterprise network.

Configuration Control

Managing device composition, versions, components, and patches to close security vulnerabilities in protection software.

Key Infrastructure

Managing cryptographic services and key infrastructure (PKI) as part of backbone infrastructure services.

Additional Security Functions

1

Event Logging

Setting up log outputs, controlling detail levels, and managing event composition for comprehensive logging.

2

Security Auditing

Obtaining and evaluating objective data on current IP security state, analyzing logs, and searching for intruders.

3

Real-Time Monitoring

Providing information about device status, activity, and security events including potential attacks.

4

Design & Inventory

Determining installation points, accounting for protective equipment, and monitoring device status.

Two Integration Approaches

Embedded Security

Companies: Cisco Systems, Computer Associates, Hewlett Packard, Tivoli Systems

Approach: Integrate security management into traditional network management systems

Drawbacks: High cost and some security aspects remain outside system scope

Specialized Platforms

Companies: Check Point Software Technologies (OSM)

Approach: Dedicated security management solutions focused solely on security problems

Benefits: Centralized policy management across devices from various manufacturers

Key Management Principles

Centralized Control

Security management must be centralized and independent of operating systems and application systems used.

Unified Logging

Event recording systems should be unified so administrators can compose a complete picture of CIS changes.

Vertical Infrastructure

Common infrastructures like PKI and X.500 directories prevent data duplication and ensure synchronization across systems.

Essential Vertical Infrastructures

PKI Infrastructure

Public key management using identity certificates and credential certificates for flexible access control.

Directories

User identifiers and information required by access control systems, often containing policies and certificates.

Authentication Systems

RADIUS, TACACS, and TACACS+ servers for verifying user identities across the network.

Logging & Monitoring

Event logging, monitoring, and audit systems for comprehensive security oversight.

Global Security Management (GSM)

The GSM concept enables integrated enterprise security management with centralized, policy-based control.

Unified Policy Management

All protective equipment managed through enterprise security policy, ensuring integrity and consistency across all resources.

Single Directory

All enterprise resources defined through a distributed directory, updatable via LDAP protocol integration.

Centralized Control

Policy-based management of local information protection tools from a central authority.

Global vs. Local Security Policy

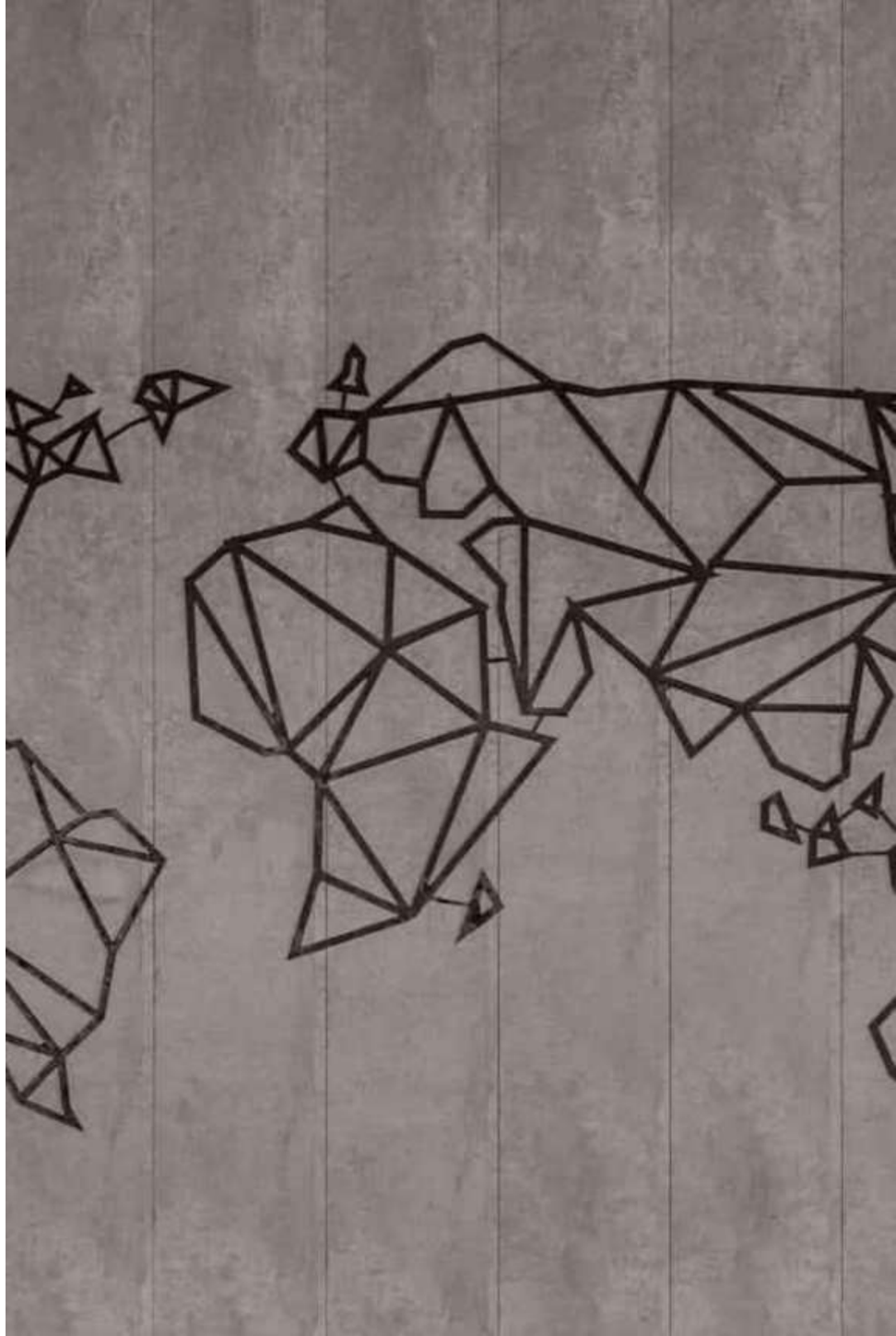
Global Security Policy (GSP)

A finite set of security rules describing interaction parameters of corporate network objects:

- Required security services for connections
- Direction of security service provision
- Authentication and key exchange rules
- Event logging and alarm signaling rules

Local Security Policy (LSP)

Individual device policies automatically formed from GSP analysis and network topology. LSP broadcasting ensures coordinated execution across heterogeneous protection devices from different manufacturers.



TrustWorks System Architecture

01

Trusted GSM Console

Administrator workplace for managing security policies. Multiple consoles can be installed per GSM server, each configured for specific administrator roles.

02

Trusted GSM Server

Central control center storing global security policies, broadcasting policies to local devices, and controlling all agent states. Supports up to 65,535 distributed servers.

03

Trusted Agent

Local security software on terminals (clients, servers, gateways) performing authentication, access control, traffic protection, filtering, and event logging.

Trusted Agent Capabilities

Core Security Functions

- Authentication of security policy objects
- User definition and event tracking
- Centralized management and access control
- Traffic protection, filtering, and authentication

Advanced Features

- Multiple cryptographic service modules
- Single Sign-On (SSO) management
- Traffic compression (IPcomp)
- Network QoS reservation management
- Local anti-virus protection

The adaptive network security management model enables timely threat response by eliminating vulnerabilities and analyzing conditions that lead to their emergence.

Review questions:

1. List five main tasks of an enterprise-wide network security management system mentioned in the text.
2. Describe the two main approaches for integrating security management with traditional network management. What are the pros and cons of each?
3. What is the difference between a Global Security Policy (GSP) and a Local Security Policy (LSP)?
4. What are the three main structural elements of the TrustWorks security management system (Trusted Agent, GSM Server, GSM Console), and what does each one do?
5. Why are unified "vertical infrastructures" like PKI and directories important for security management?

Recommended literature list:

1. Stallings, W. (2013). *Network Security Essentials: Applications and Standards*. Pearson.

2. Tipton, H. F., & Krause, M. (2R007). *Information Security Management Handbook*. Auerbach Publications.

3. Verma, D. C. (2002). *Policy-Based Networking: Architecture and Algorithms*. New Riders Publishing.