



The Importance of Cybersecurity in Enterprise Networks

An overview of security requirements
and Checkpoint Architecture.

Table of contents

1. Security requirements in an enterprise network

1. Network Segmentation
2. Data Classification and Protection

2. Optimizing security posture with checkpoint architecture

1. Key components of the checkpoint architecture
2. State inspection and modern security

3. Case Study Global: Retail Corporation's Implementation of Checkpoint Architecture

1. Solution Implementation
2. Stateful Inspection Technology

1. Security requirements in an enterprise network

1. What is Network segmentation?

- The division of networks into segments/zones
- Each has its own security controls

Enhanced security

- Limits lateral movement
- Contains breaches
- Reduces attack surface

Regulatory Compliance

- Not just a security best practice!
Important requirement to meet security standards. PCI DSS
HIPAA

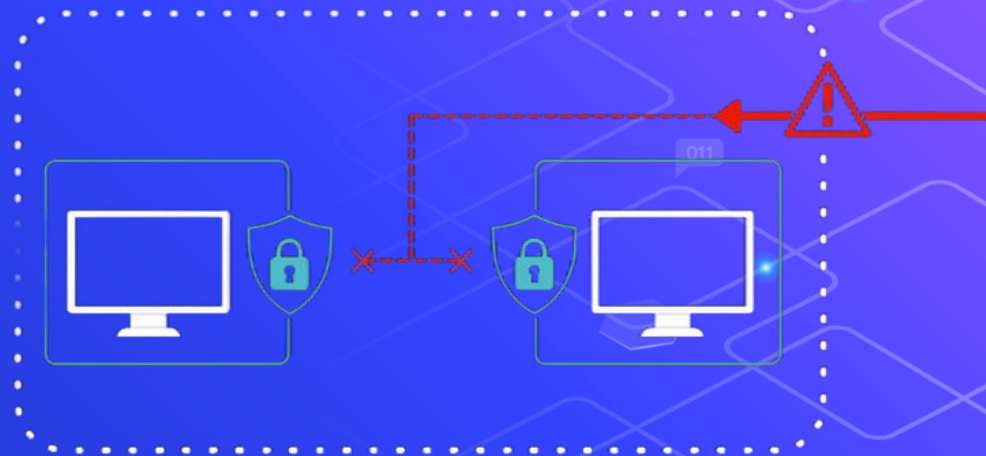


1. Security requirements in an enterprise network

1. Network segmentation

Best Practices :

- Identify critical systems and data to understand your network
- Define objectives to create plan
- Adopt a Zero trust approach, Verify and authenticate everything
- Implement strong access controls
- Regular test on the networks and update the network segmentations

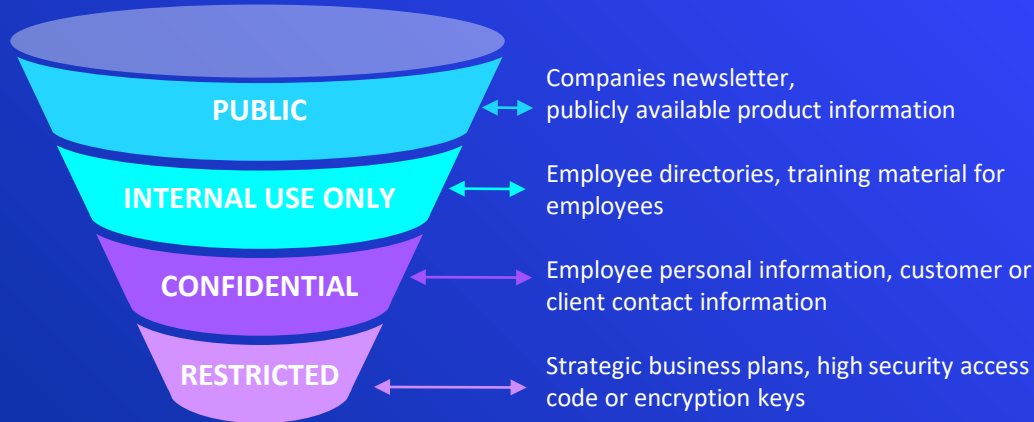


1. Security requirements in an enterprise network

2. Data classification and protection

Definition: Data classification
Process of categorizing data according to their sensitivity

Commonly used categories:



Challenges:

- Complexity & Time consuming
- Impact on collaboration and productivity

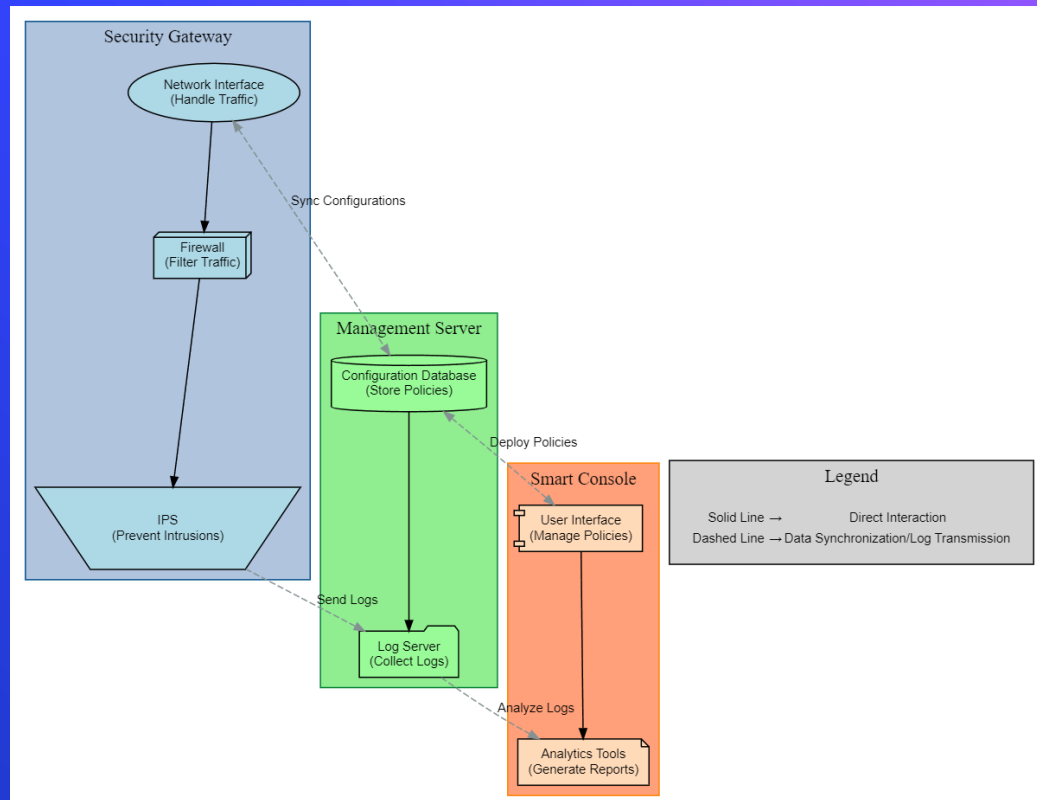
Importance:

- Mitigate risks :
 - Unauthorized access
 - Data breaches
 - Compliance violations
- Trust and company's reputation

2. Optimizing security posture with checkpoint architecture

1. Key components of the checkpoint architecture

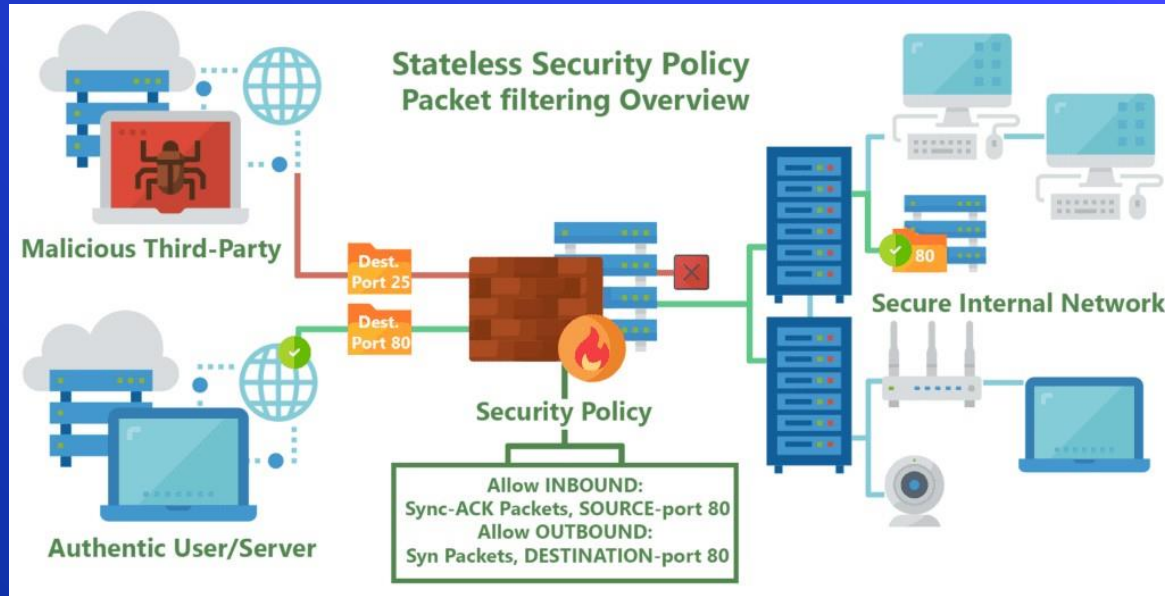
Enterprise Network Security with Checkpoint Architecture:



2. Optimizing security posture with checkpoint architecture

2. State inspection and modern security

Comparison: Traditional Filtering vs State Inspection

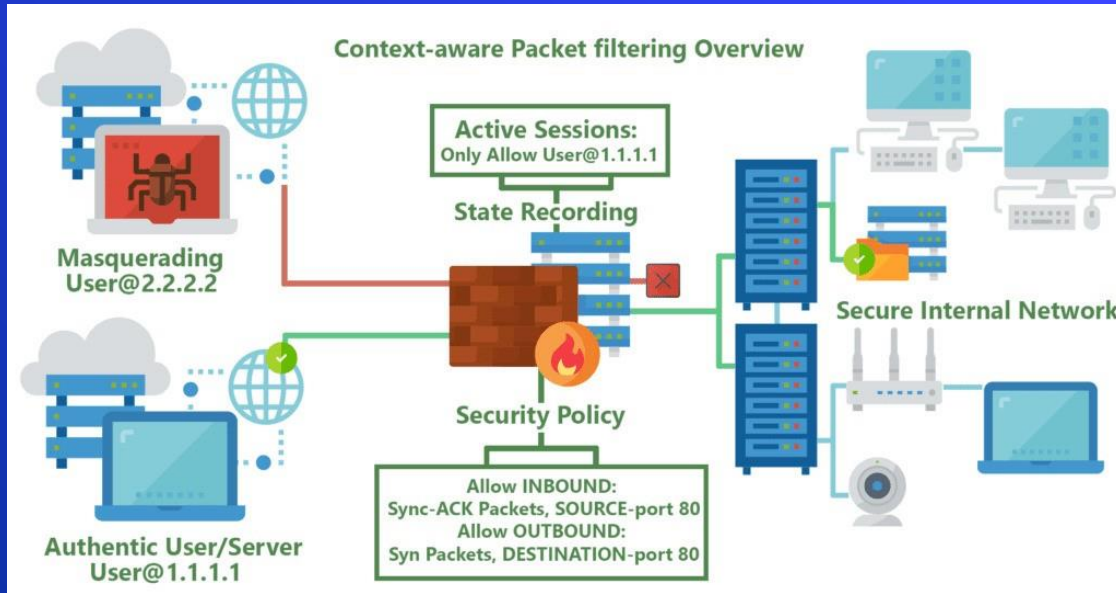


- Uses security policies to filter the packet at the packet level

2. Optimizing security posture with checkpoint architecture

2. State inspection and modern security

Comparison: Traditional Filtering vs State Inspection



- Leverages the context of the session, network policies, and the network itself to filter packets more efficiently

2. Optimizing security posture with checkpoint architecture

2. State inspection and modern security

Comparison: Traditional Filtering vs State Inspection

Which is better?

Pros

- Way more secure than traditional filtering

Cons

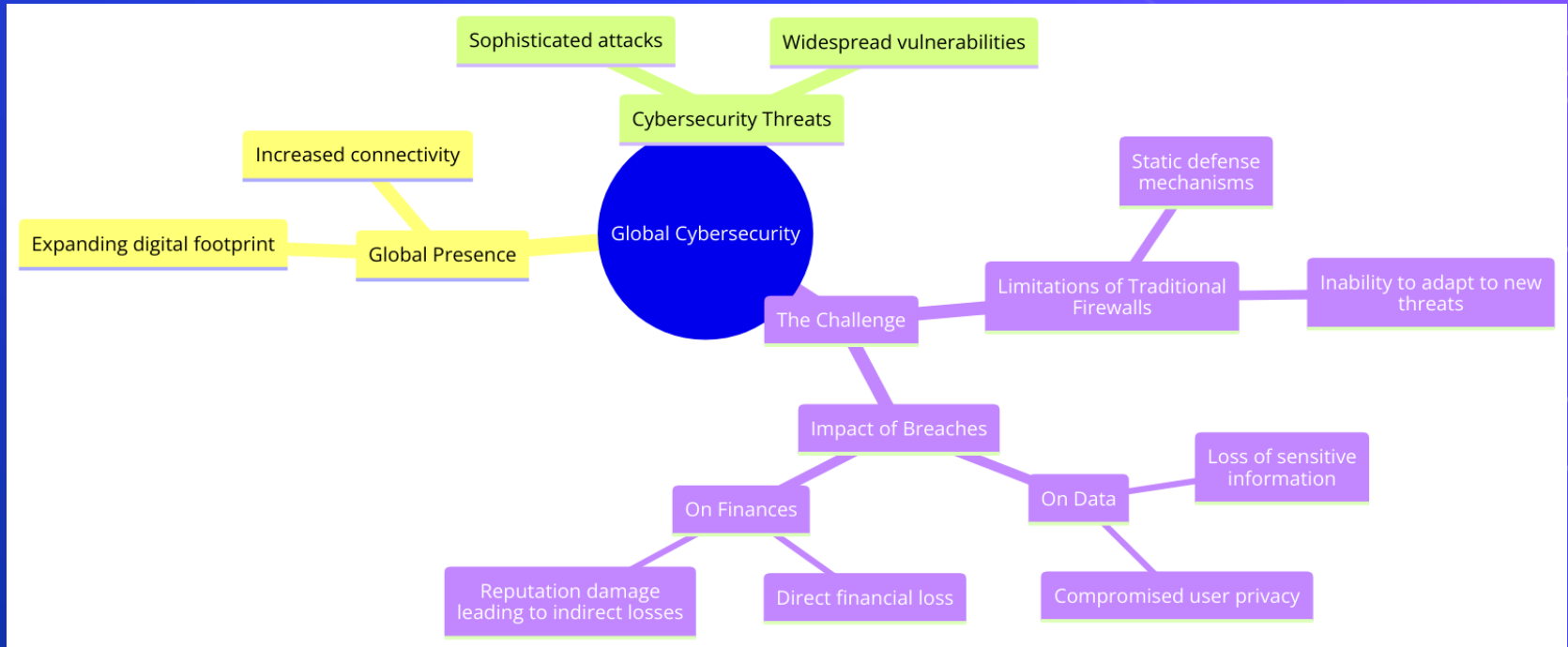
- Cost of implementation and maintenance are high (software and hardware)

3. Case Study: Global Retail Corporation's Implementation of Checkpoint Architecture



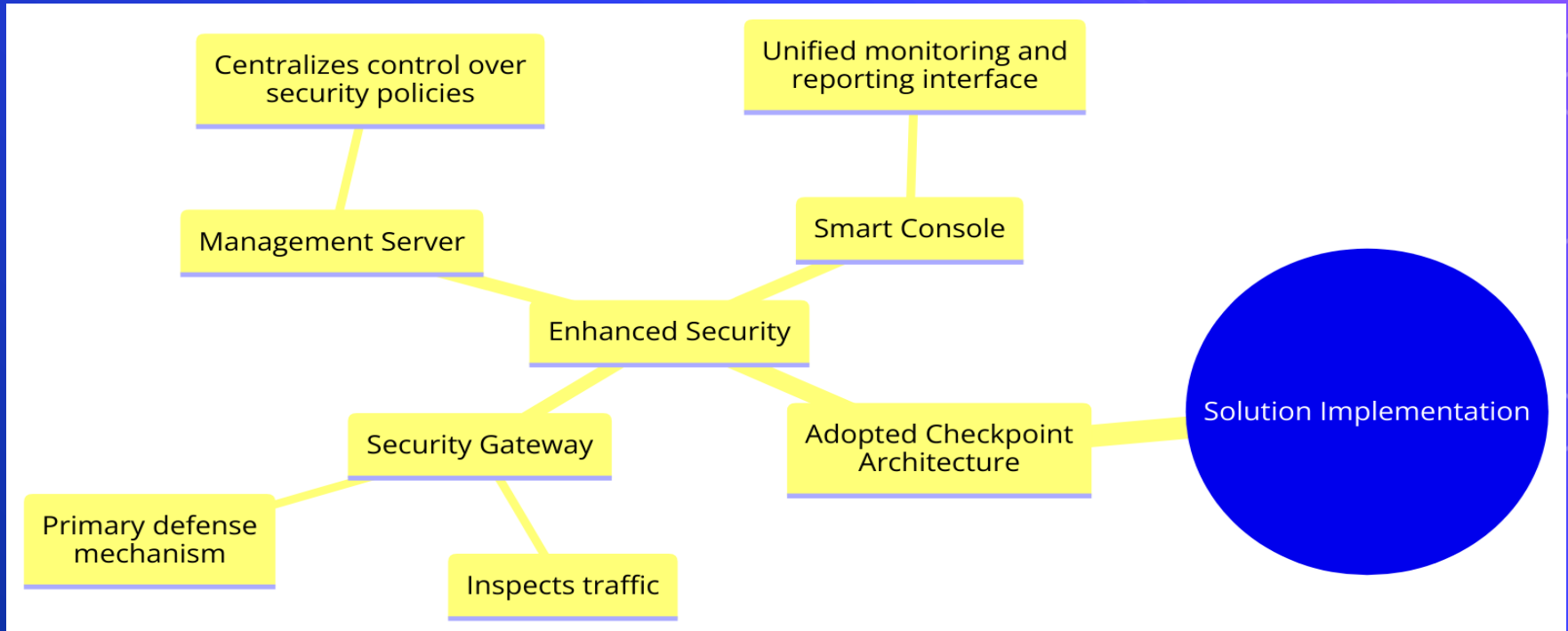
3. Case study: global retail corporation's implementation of checkpoint architecture

Context and problem faced



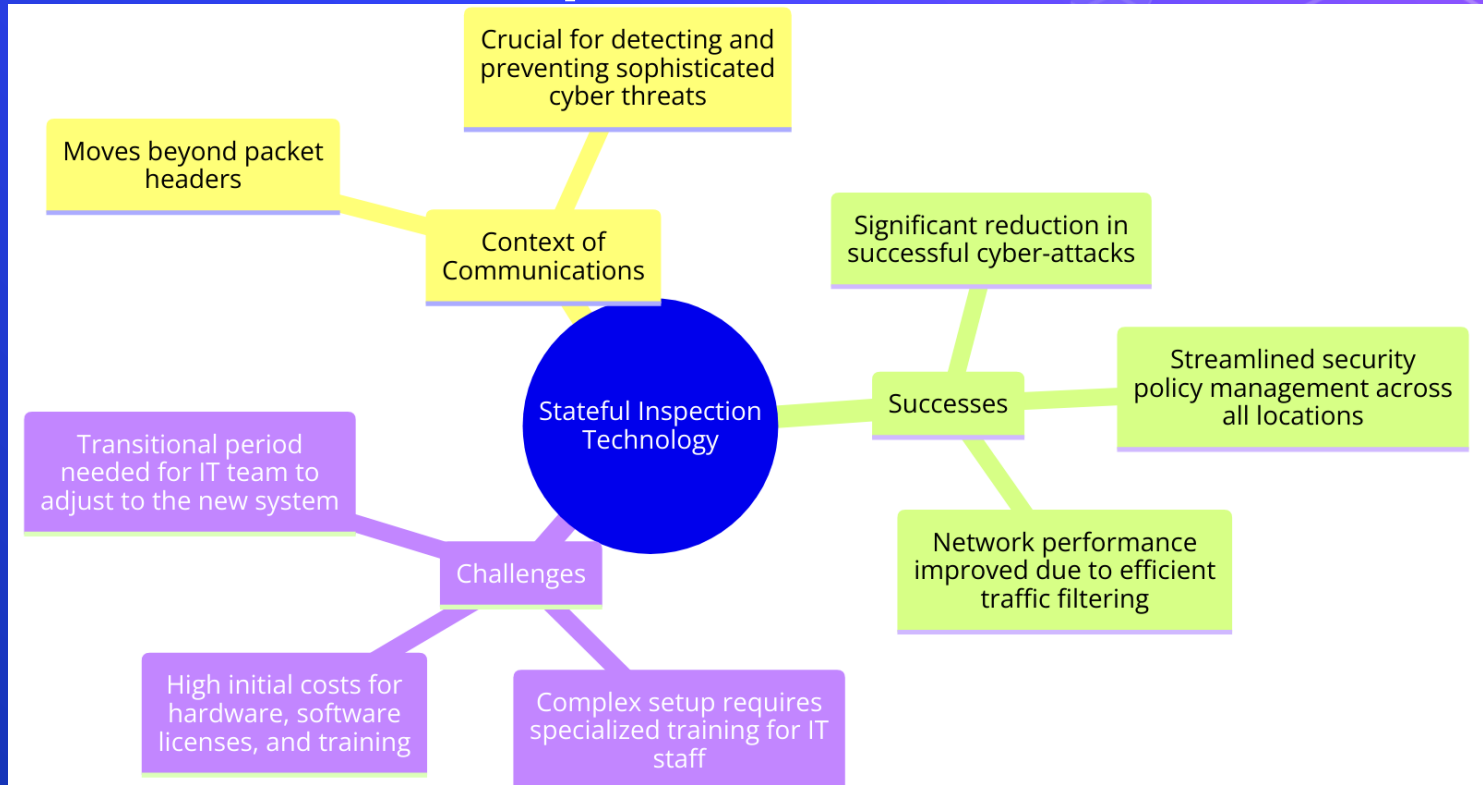
3. Case study: global retail corporation's implementation of checkpoint architecture

Solution



3. Case study: global retail corporation's implementation of checkpoint architecture

Stateful
Inspection
Technology
applied



Conclusion

- ⬡ Despite challenges, Checkpoint Architecture greatly improved security posture.
- ⬡ Benefits of advanced security measures outweigh initial hurdles.
- ⬡ Effective protection against evolving cyber threats demonstrated.

References

⬡ Stateless VS Stateful Packet

<https://www.lanner-america.com/blog/stateless-vs-stateful-packet-filtering-firewalls-better/>

⬡ The Global Retail Company case study

<https://nordcloud.com/case-studies/global-retail-company/>

⬡ Network segmentation

<https://www.comptia.org/blog/security-awareness-training-network-segmentation>