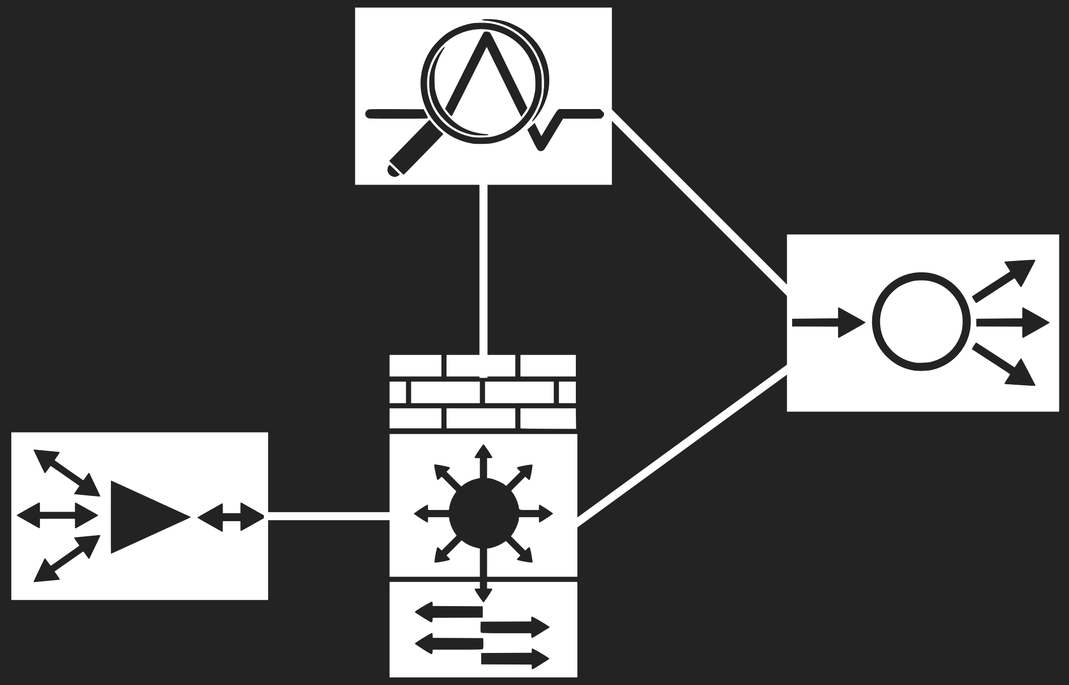
Don’t Yank My Chain

Auditable NF Service Chaining

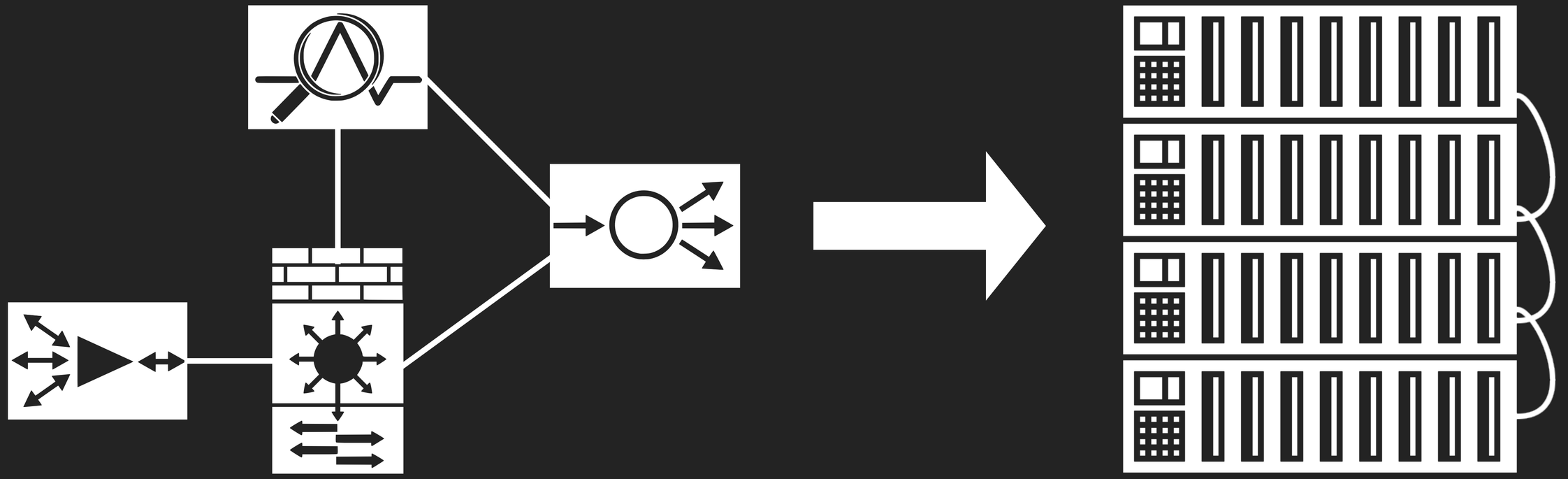
Guyue Liu, **Hugo Sadok**, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, Justine Sherry

Carnegie Mellon University

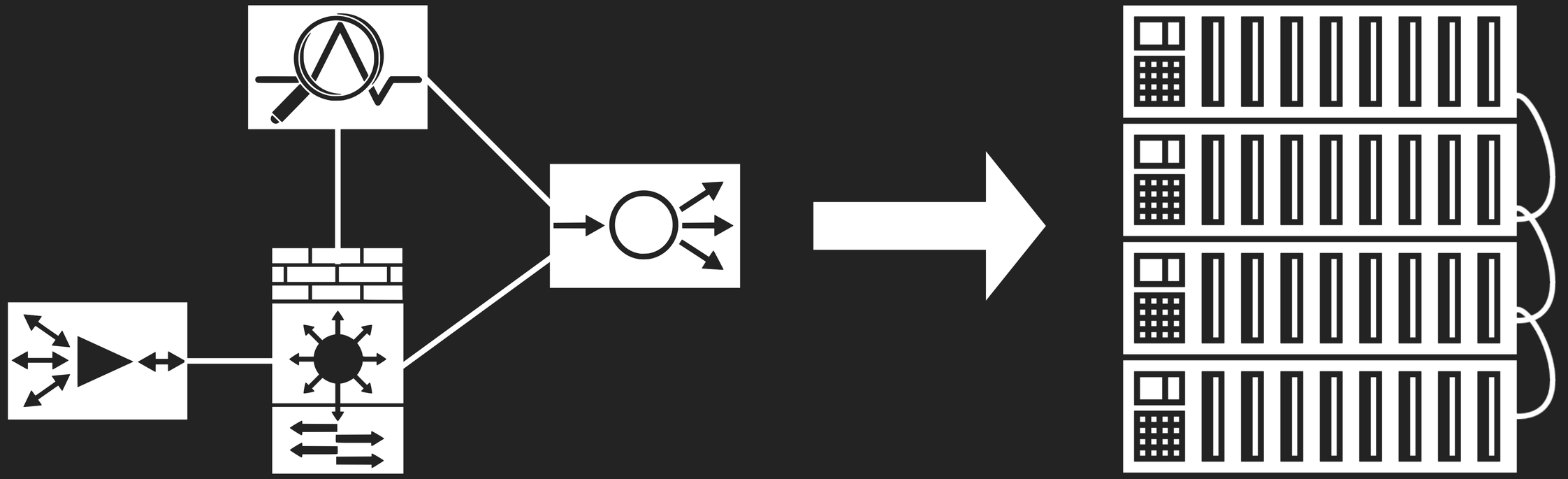
Network Function Virtualization (NFV)



Network Function Virtualization (NFV)

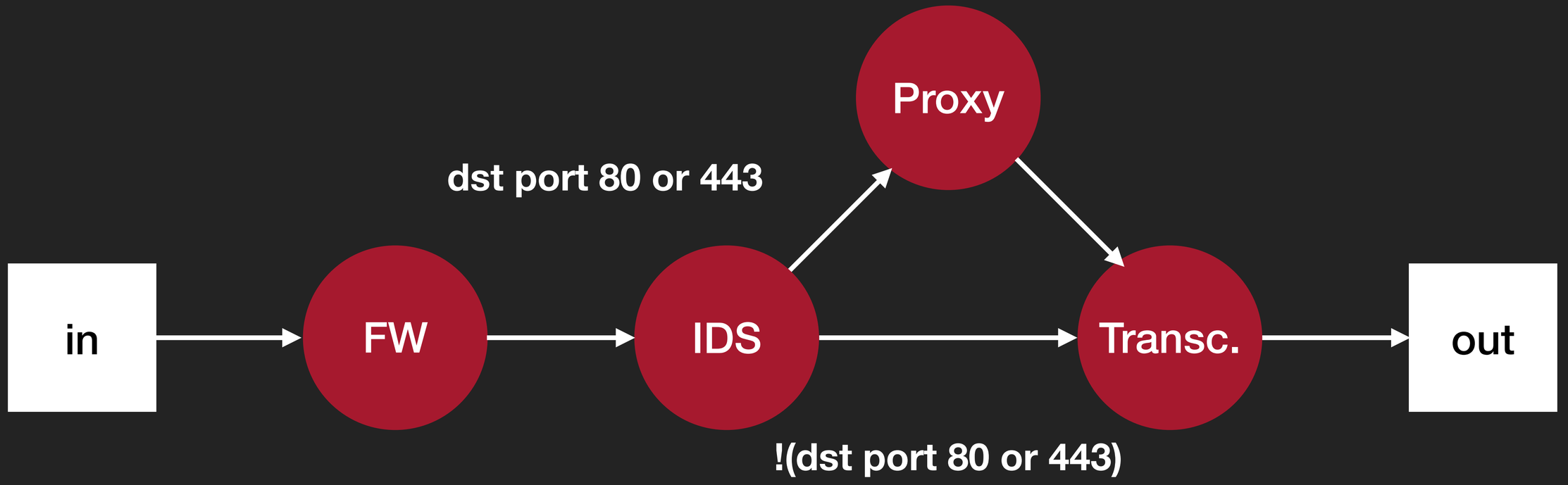


Network Function Virtualization (NFV)



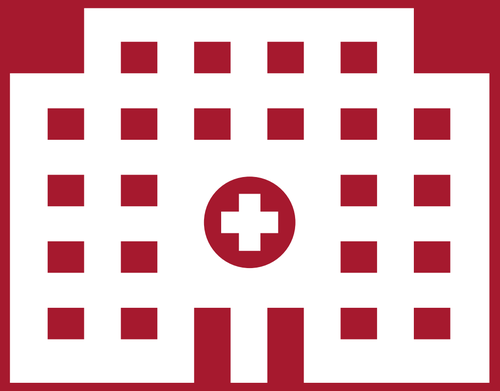
Benefits: ① Cost ② Elasticity ③ Richer Policies

Policies in NFV



Policy Graph

NFs are mandated by legal and policy requirements



HIPPA

PCI

FERPA

Regulatory Compliance (NIST 800-53)*

Regulatory Compliance (NIST 800-53)*

*There is also ISO 270001, which is an equivalent international standard

Regulatory Compliance (NIST 800-53)*

Periodically test that the infrastructure is running properly

*There is also ISO 270001, which is an equivalent international standard

Regulatory Compliance (NIST 800-53)*

Periodically test that the infrastructure is running properly

System must provide **logs** of anomalies and past behavior

*There is also ISO 270001, which is an equivalent international standard

Regulatory Compliance (NIST 800-53)*

Periodically test that the infrastructure is running properly

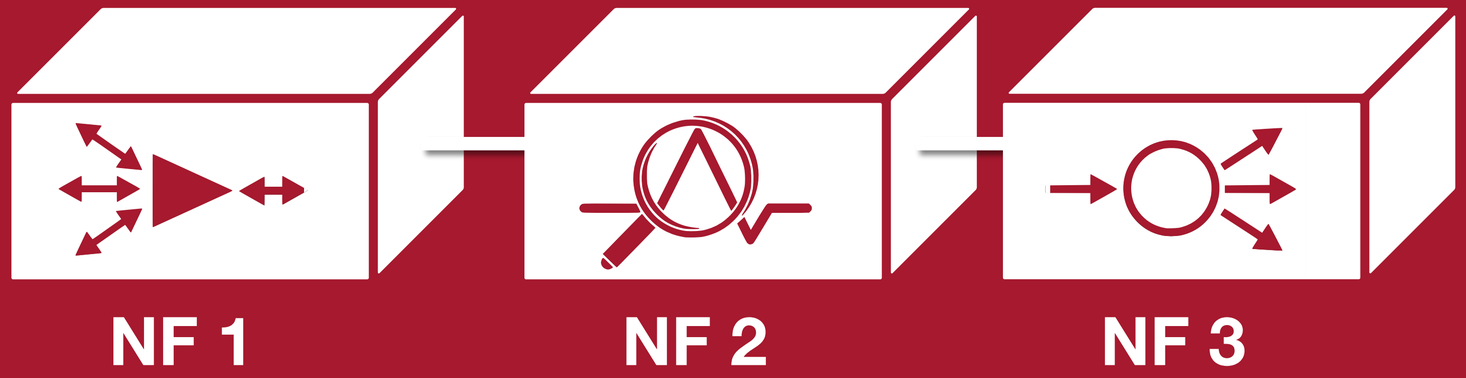
System must provide **logs** of anomalies and past behavior

Independent auditors must verify that security mechanisms are in place and running correctly

*There is also ISO 270001, which is an equivalent international standard

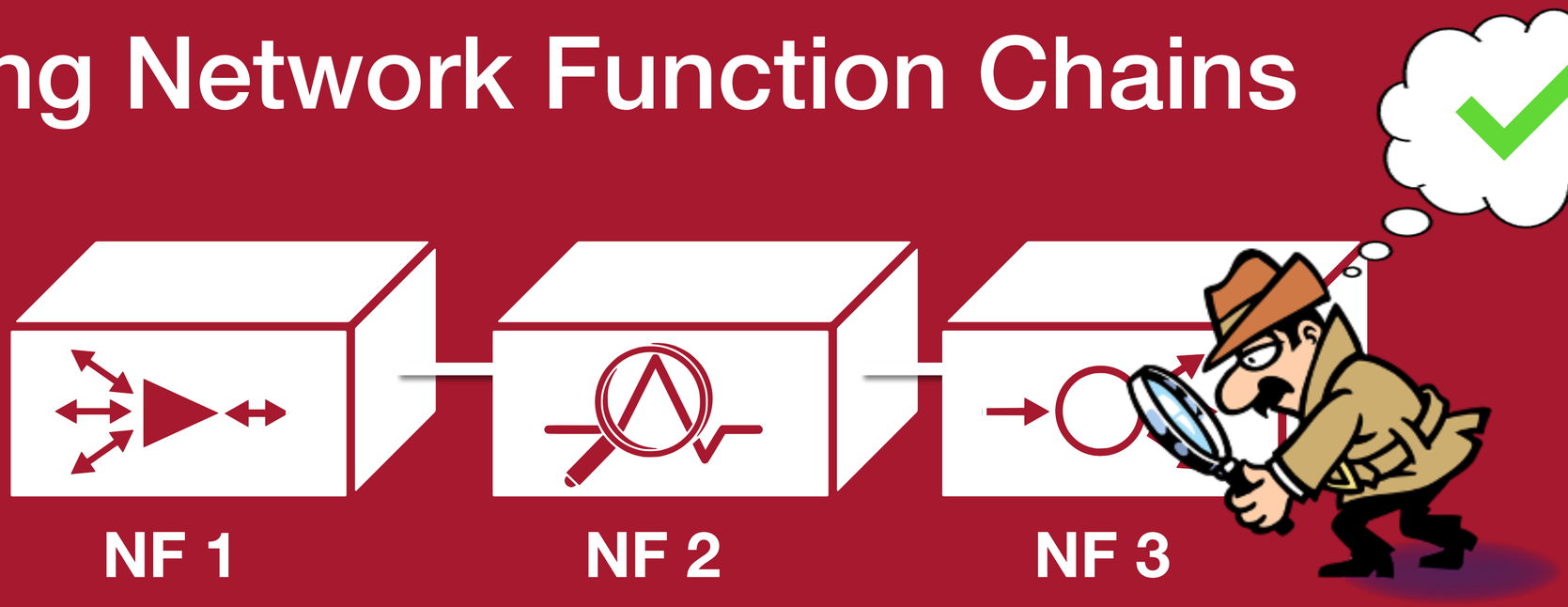
Auditing Network Function Chains

Traditional Network



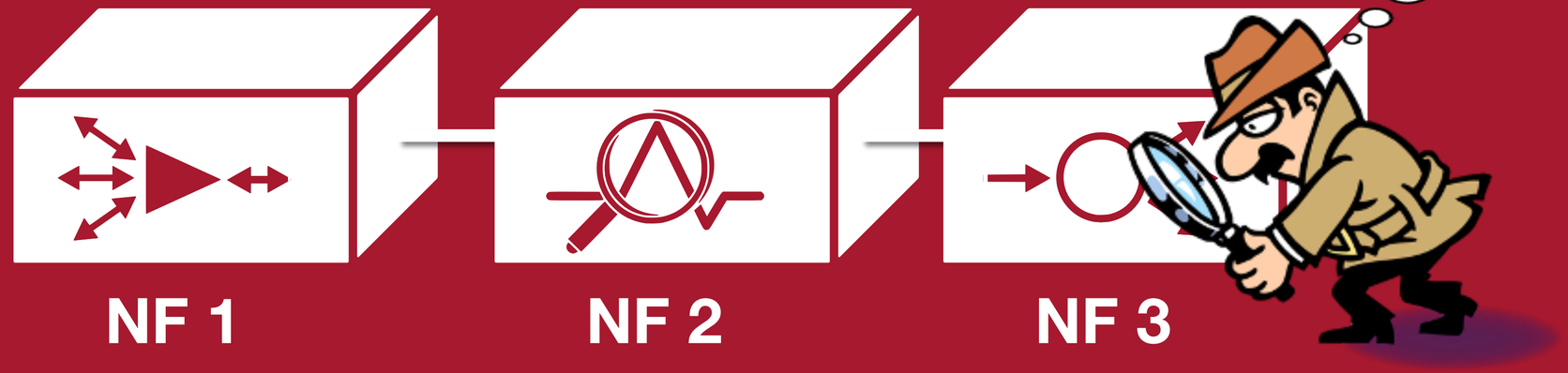
Auditing Network Function Chains

Traditional Network

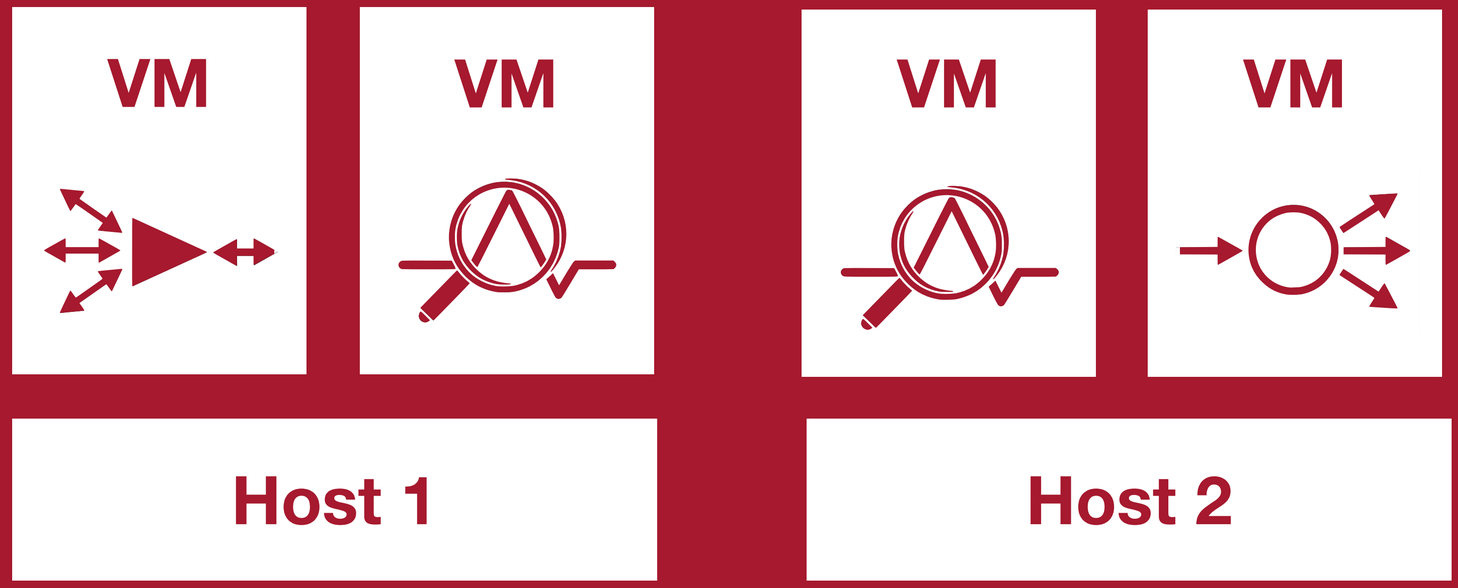


Auditing Network Function Chains

Traditional Network

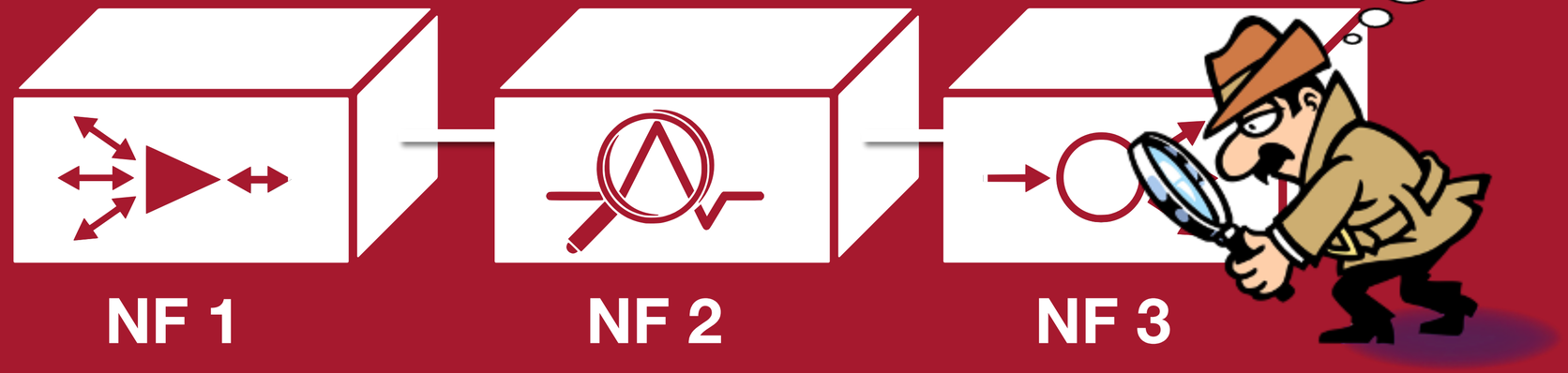


NFV



Auditing Network Function Chains

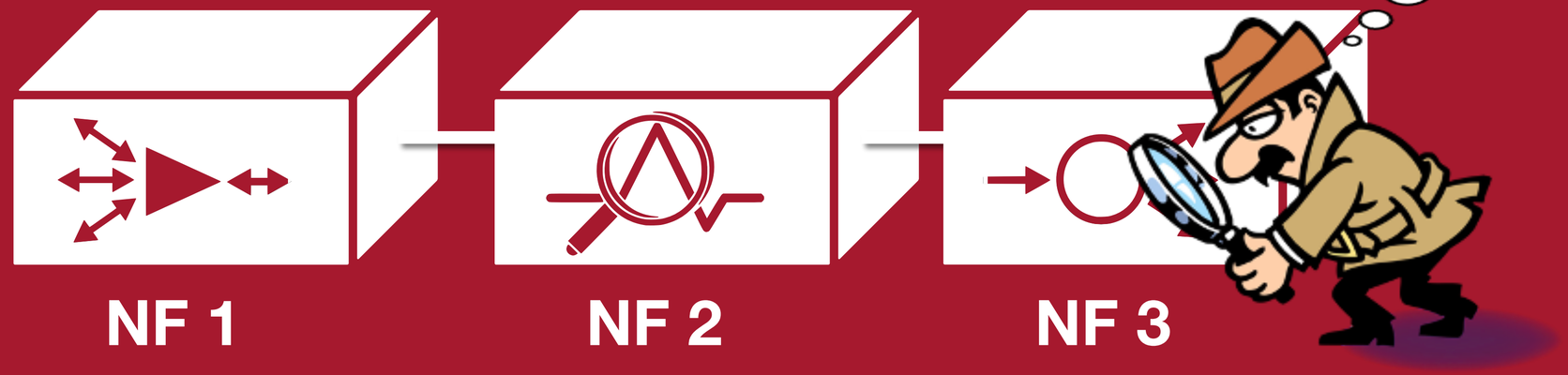
Traditional Network



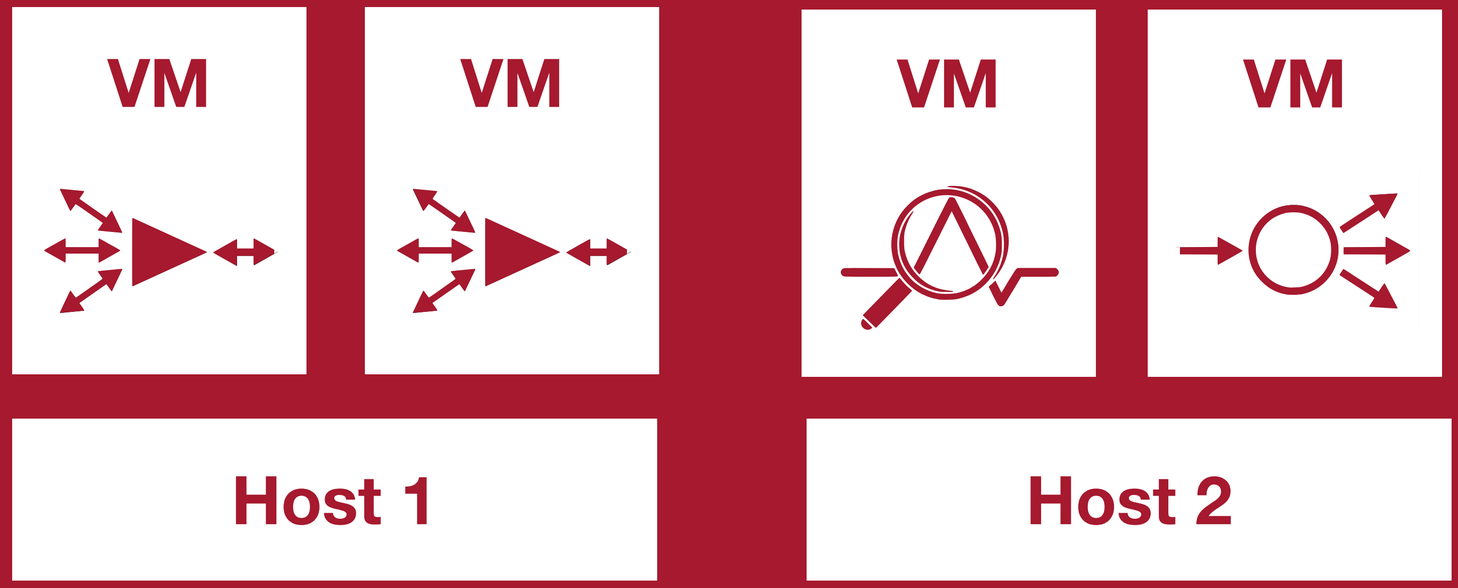
NFV

Auditing Network Function Chains

Traditional Network

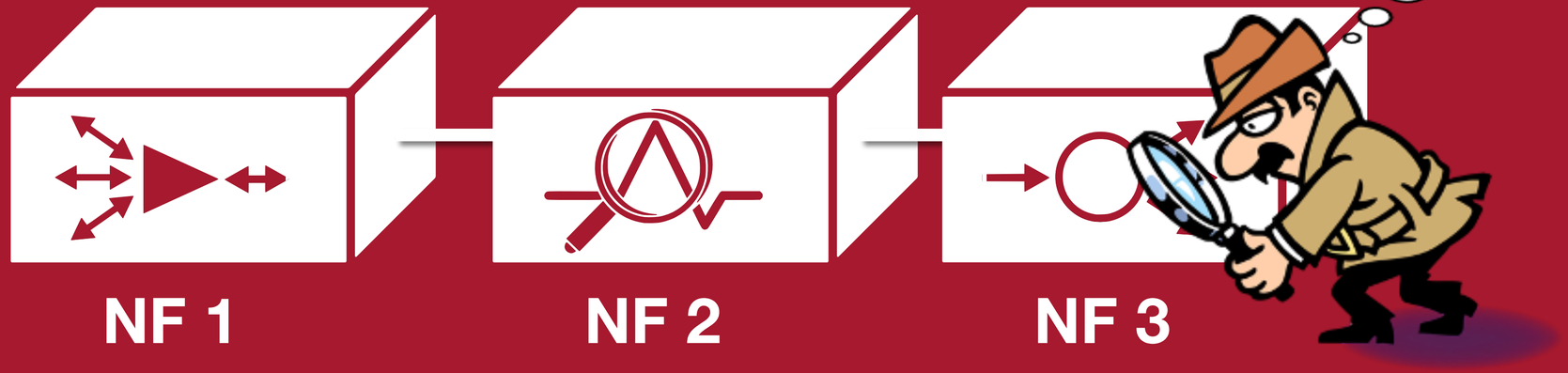


NFV

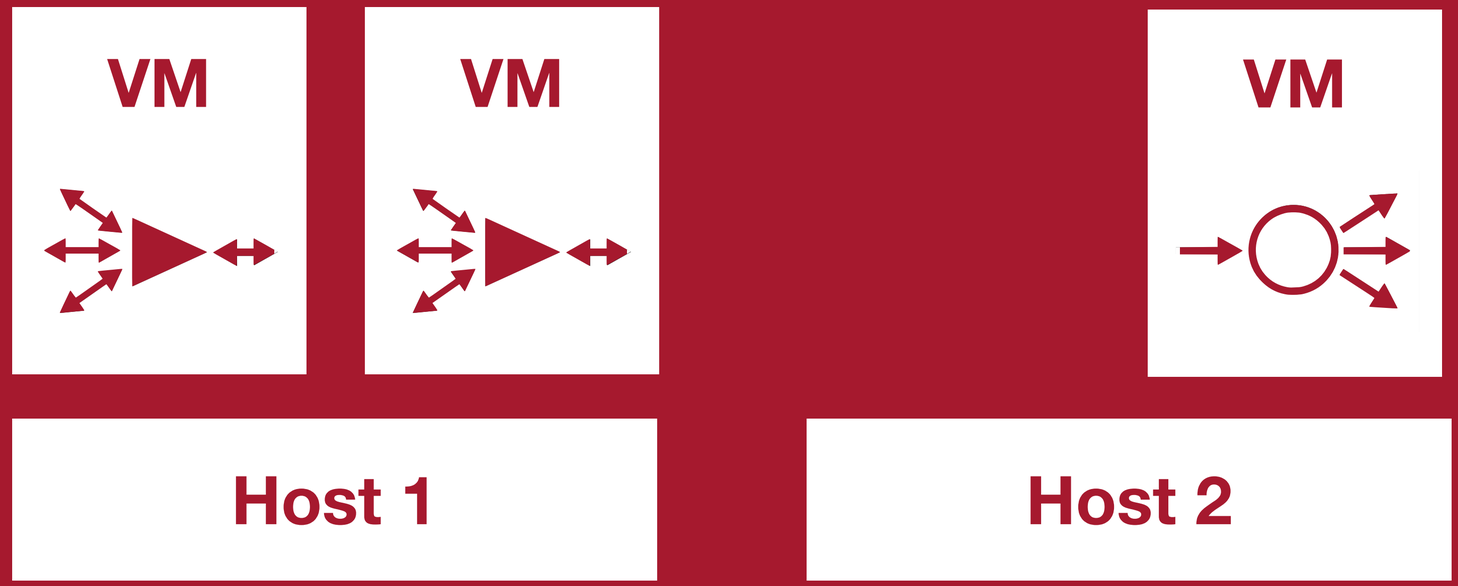


Auditing Network Function Chains

Traditional Network

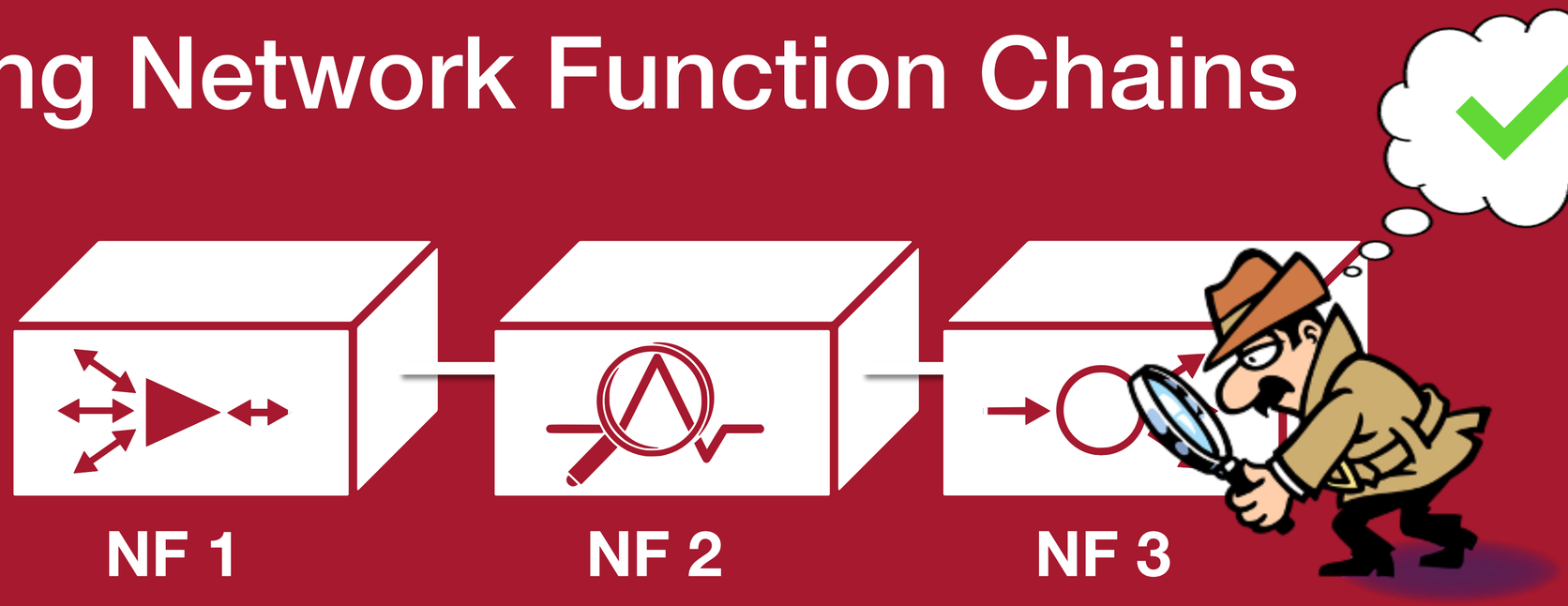


NFV

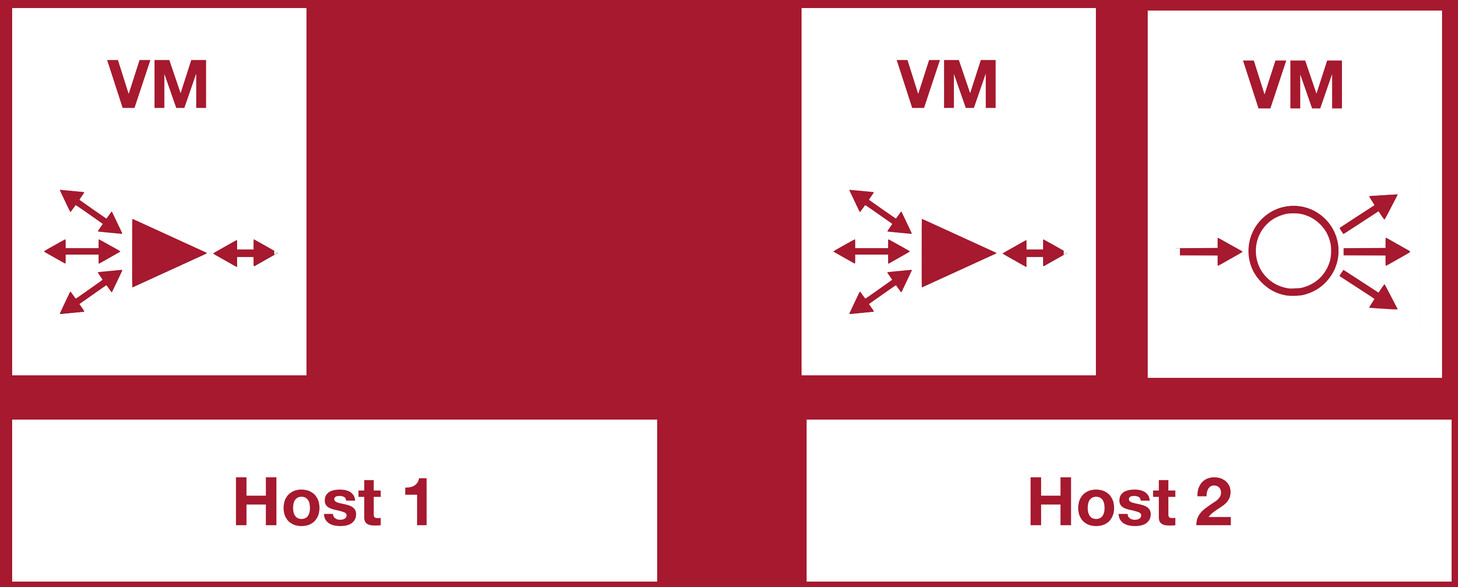


Auditing Network Function Chains

Traditional Network

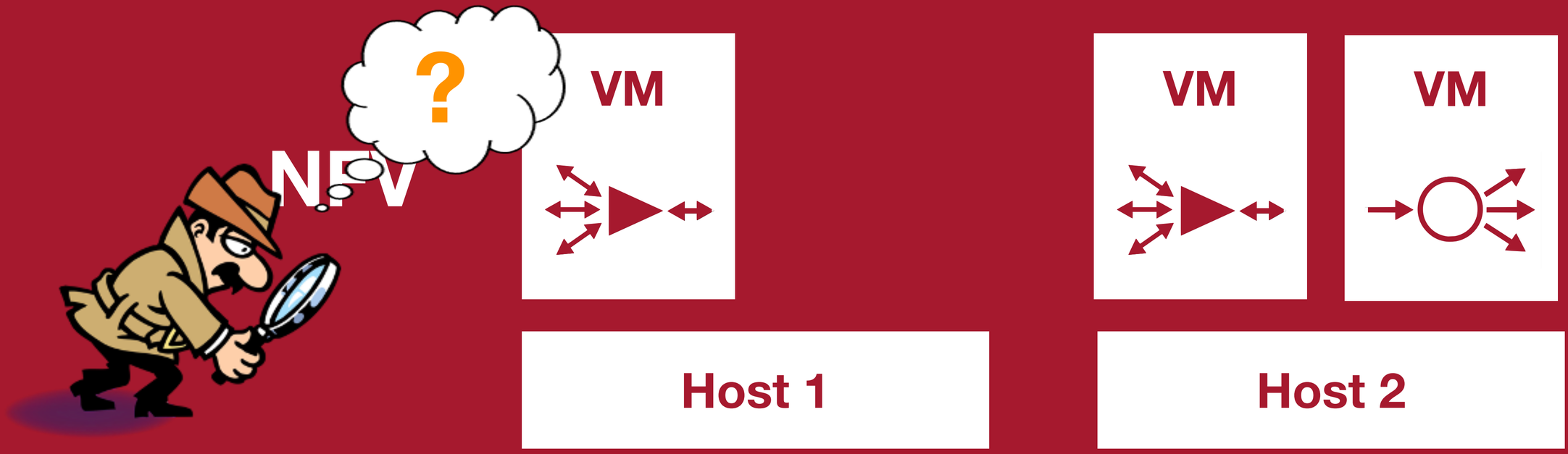


NFV



Auditing Network Function Chains

Traditional Network



Traditional networks

① Auditors can rely on the network topology to ensure that the correct NF chain is being used

② Auditors can inspect and approve HW boxes

③ Auditors can trust logs captured by the HW boxes

Traditional networks

① Auditors can rely on the network topology to ensure that the correct NF chain is being used

② Auditors can inspect and approve HW boxes

③ Auditors can trust logs captured by the HW boxes

NFV

Traditional networks

① Auditors can rely on the network topology to ensure that the correct NF chain is being used

② Auditors can inspect and approve HW boxes

③ Auditors can trust logs captured by the HW boxes

NFV

① NF chains are dynamic

Traditional networks

① Auditors can rely on the network topology to ensure that the correct NF chain is being used

② Auditors can inspect and approve HW boxes

③ Auditors can trust logs captured by the HW boxes

NFV

① NF chains are dynamic

② Software NFs can be modified by an attacker

Traditional networks

① Auditors can rely on the network topology to ensure that the correct NF chain is being used

② Auditors can inspect and approve HW boxes

③ Auditors can trust logs captured by the HW boxes

NFV

① NF chains are dynamic

② Software NFs can be modified by an attacker

③ Logs stored in the server can be tampered with

These limitations are not fundamental to NFV

These limitations are not fundamental to NFV

With AuditBox for NFV, auditors have even stronger auditing guarantees than traditional NF deployments

AuditBox

AuditBox

Provides auditing capabilities to NFV deployments

AuditBox

Provides auditing capabilities to NFV deployments

① **NF functionality cannot be modified/manipulated**

② **Traffic is steered between NFs according to the administrator's policy**

③ **Provide logs that attest that the correct policy is being followed**

④ **Good performance**

AuditBox

Key Techniques:

① Secure Enclaves

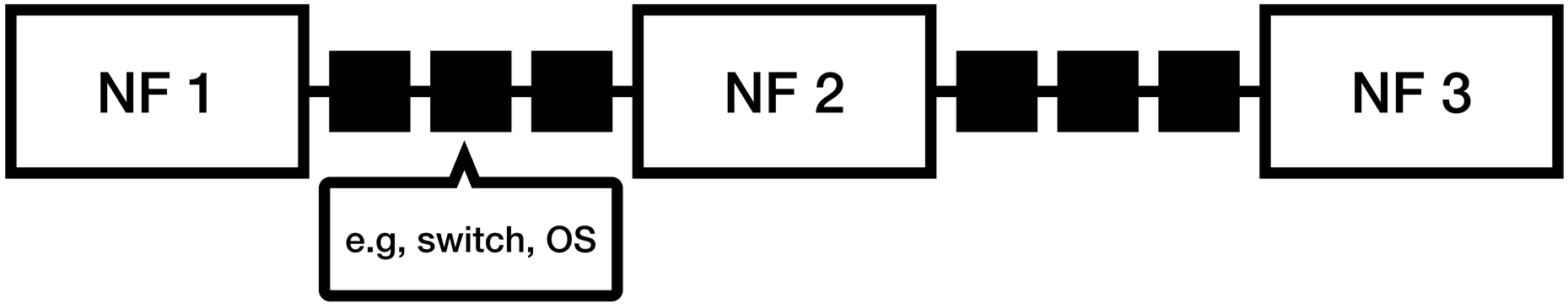
② NF Hop-by-Hop Updated Attestation

③ Secret Logging

④ Efficient Crypto Mechanisms

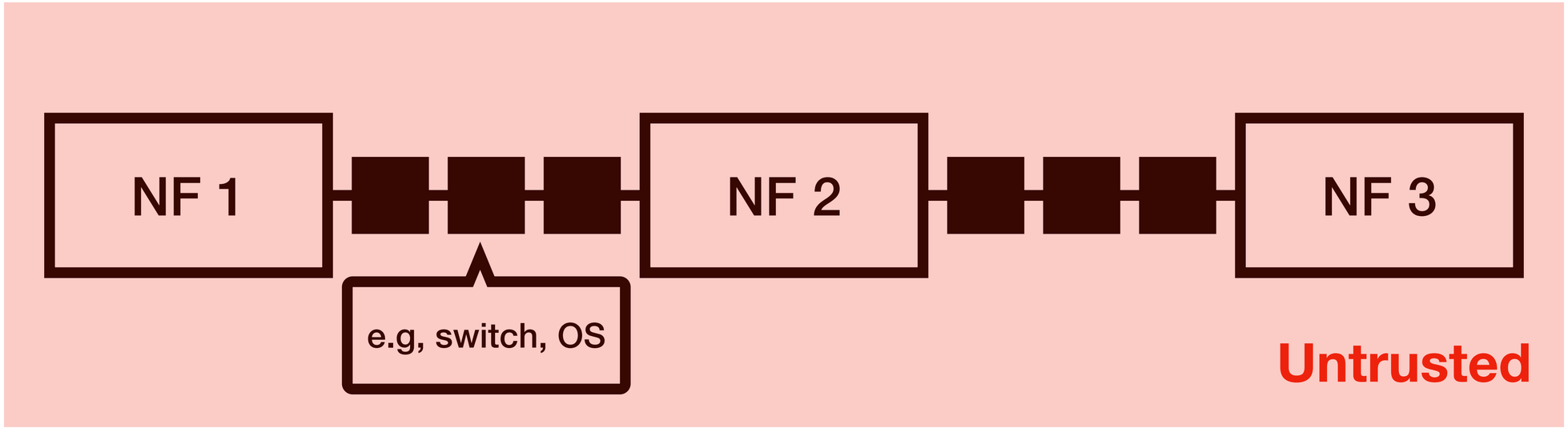
① Secure Enclaves

Logical view of an NF chain



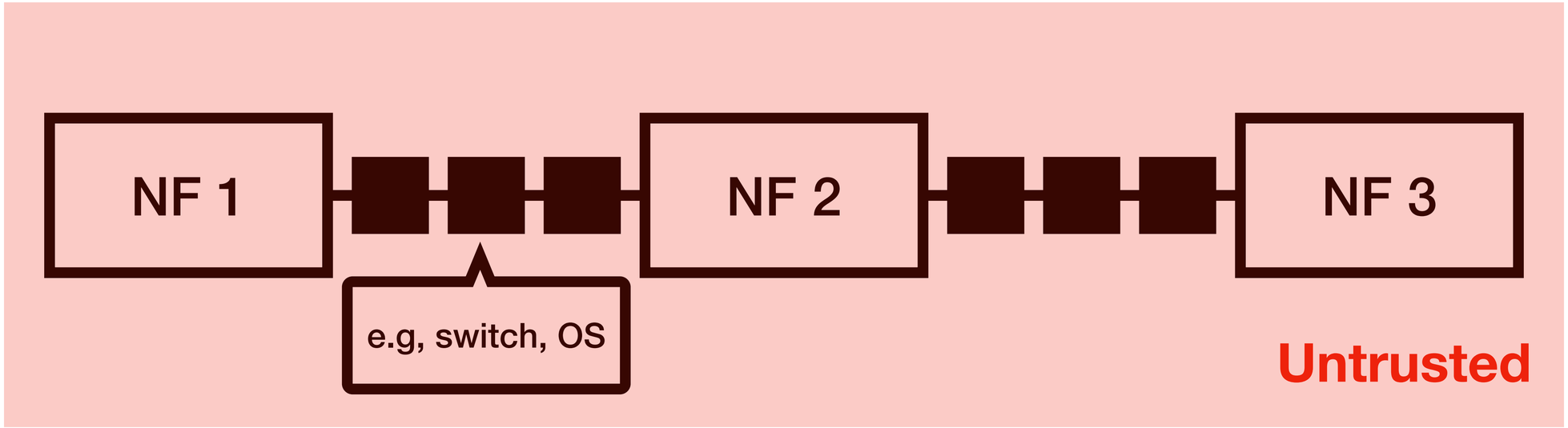
① Secure Enclaves

Logical view of an NF chain



① Secure Enclaves

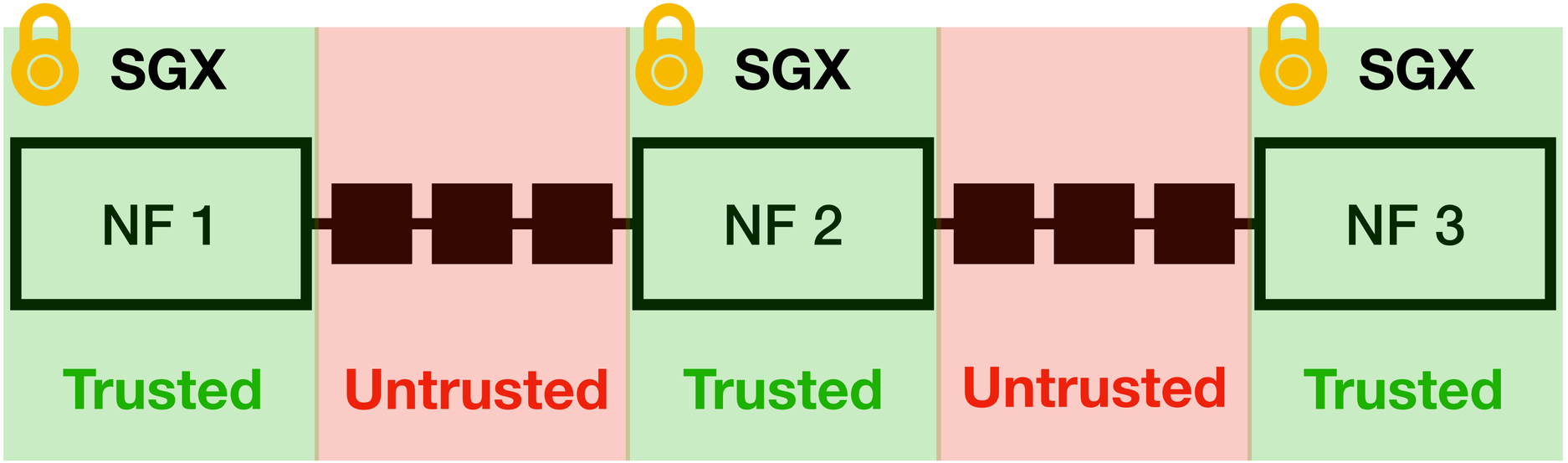
Logical view of an NF chain



Need to attest that all components in the path are correct

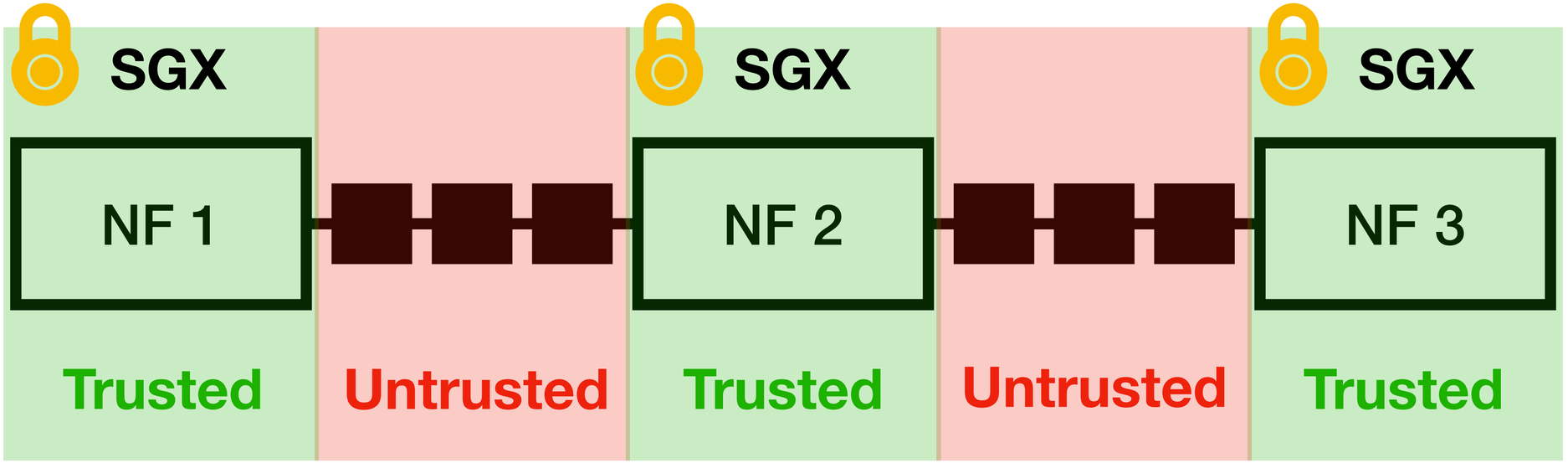
① Secure Enclaves

Run NFs inside secure enclaves (e.g., Intel SGX)



① Secure Enclaves

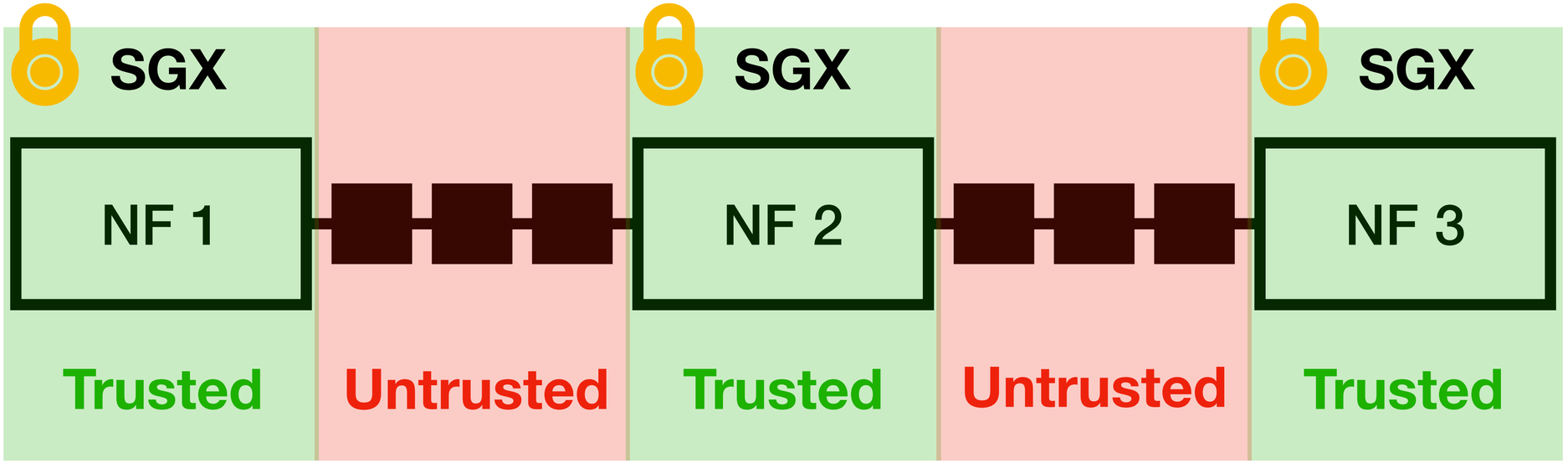
Run NFs inside secure enclaves (e.g., Intel SGX)



- Auditors have guarantees that the audited NF software is running

① Secure Enclaves

Run NFs inside secure enclaves (e.g., Intel SGX)



- Auditors have guarantees that the audited NF software is running
- Remaining untrusted functionality is responsible for packet forwarding

Verified Routing Protocols (VRPs)

Examples: EPIC [USENIX '20], OPT [SIGCOMM '14], ICING [CoNEXT ’11]

Verified Routing Protocols (VRPs)

Examples: EPIC [USENIX '20], OPT [SIGCOMM '14], ICING [CoNEXT ’11]

VRP Assumptions:

NFV Needs:

Verified Routing Protocols (VRPs)

Examples: EPIC [USENIX '20], OPT [SIGCOMM '14], ICING [CoNEXT ’11]

VRP Assumptions:

Immutable Packets

NFV Needs:

Mutable Packets

Verified Routing Protocols (VRPs)

Examples: EPIC [USENIX '20], OPT [SIGCOMM '14], ICING [CoNEXT ’11]

VRP Assumptions:

- Immutable Packets
- Pre-known Paths

NFV Needs:

- Mutable Packets
- Dynamic Paths

Verified Routing Protocols (VRPs)

Examples: EPIC [USENIX '20], OPT [SIGCOMM '14], ICING [CoNEXT ’11]

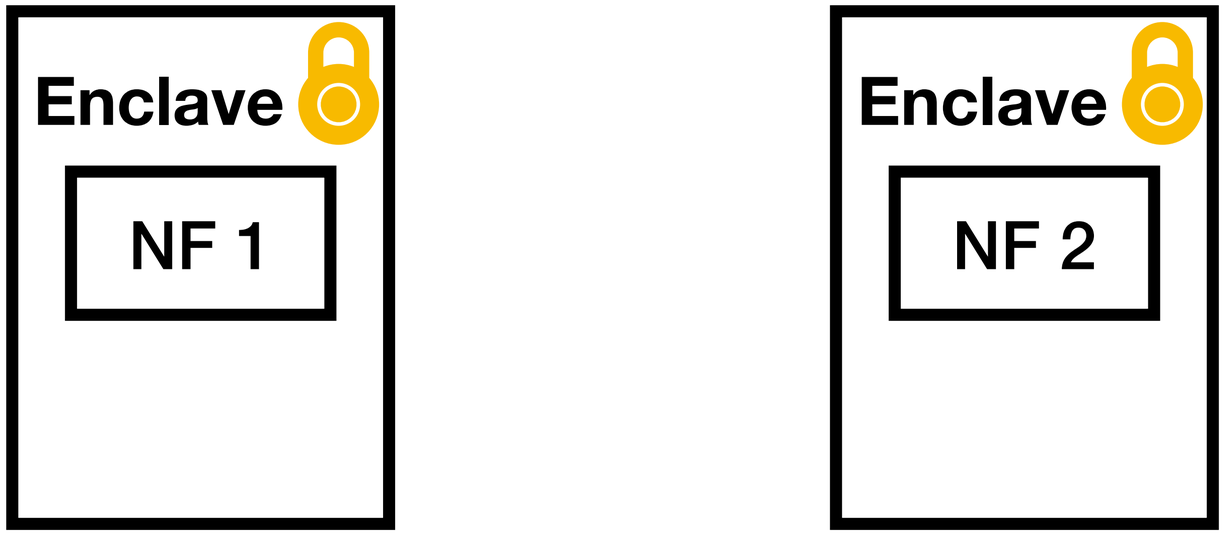
VRP Assumptions:

- Immutable Packets
- Pre-known Paths
- Stateless Processing Nodes

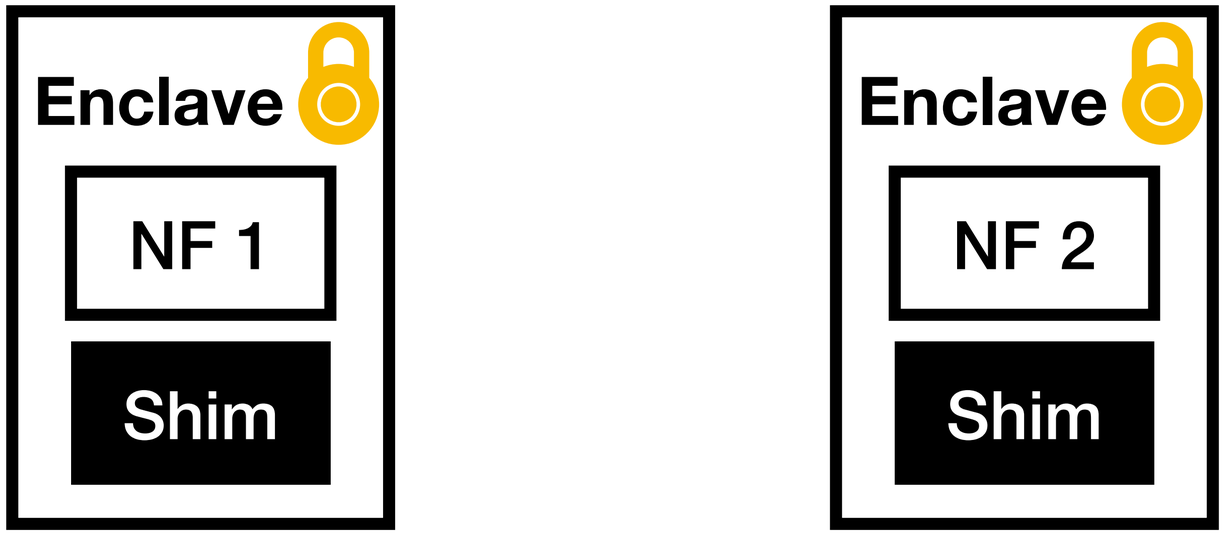
NFV Needs:

- Mutable Packets
- Dynamic Paths
- Stateful Processing Nodes

② NF Hop-by-Hop Updated Attestation

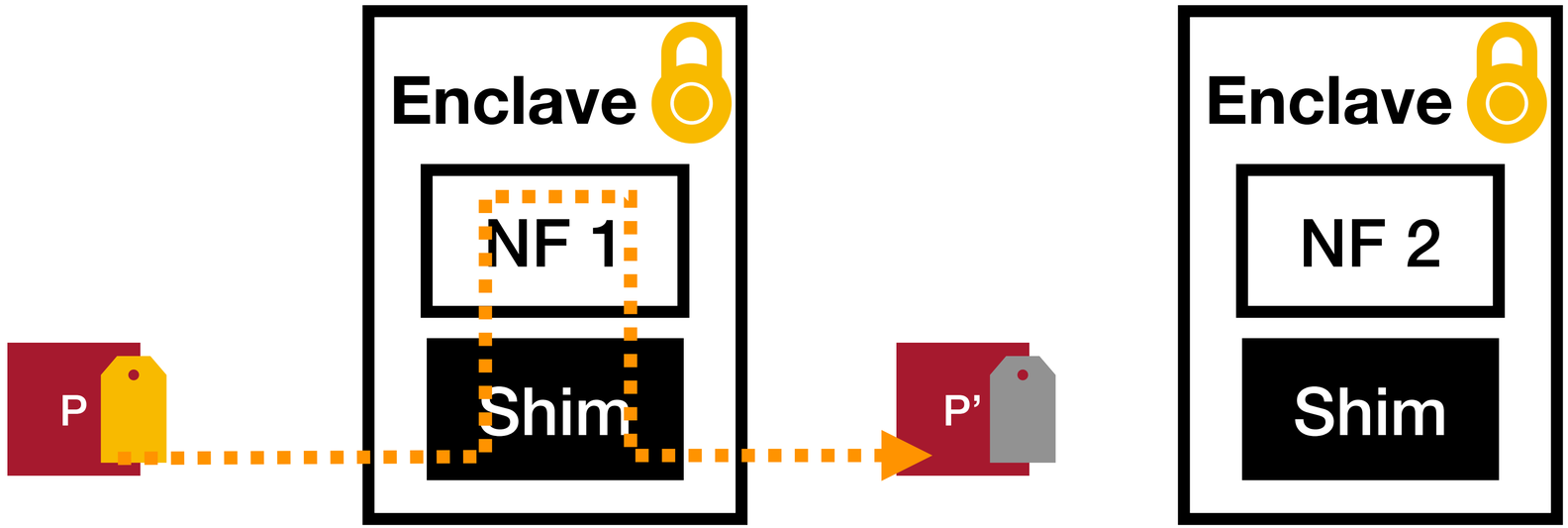


② NF Hop-by-Hop Updated Attestation



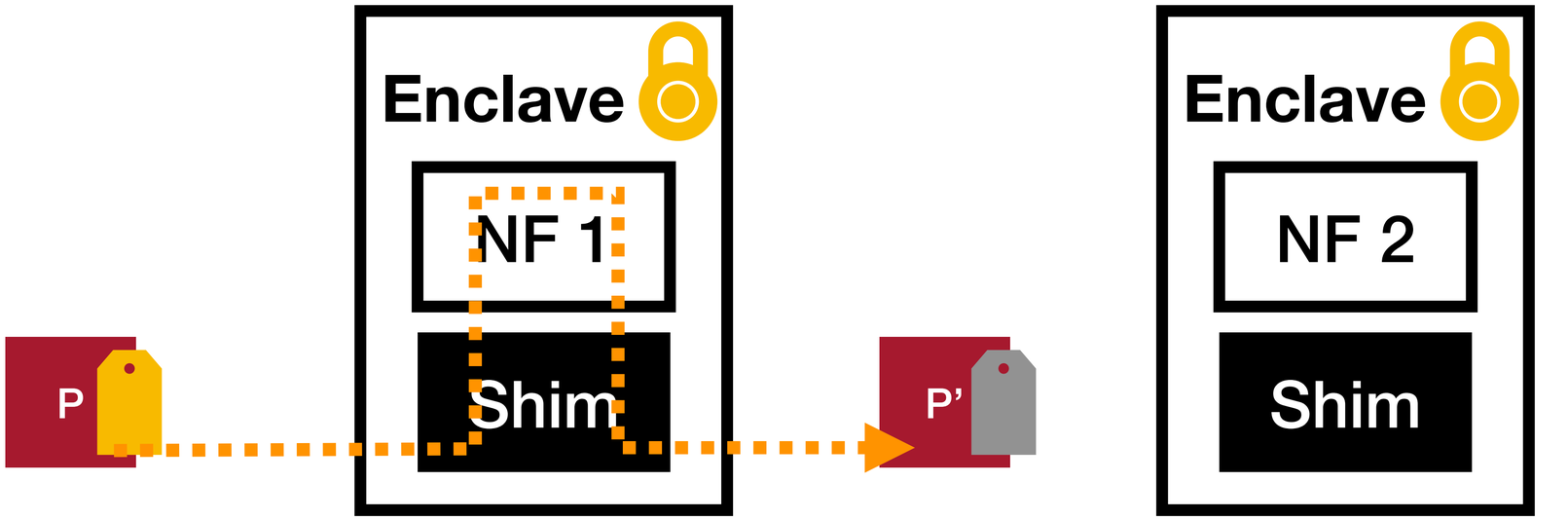
- A **shim** in every enclave mediates all incoming and outgoing packets

② NF Hop-by-Hop Updated Attestation



- A **shim** in every enclave mediates all incoming and outgoing packets
- Attestation happens between **pairs of shims**

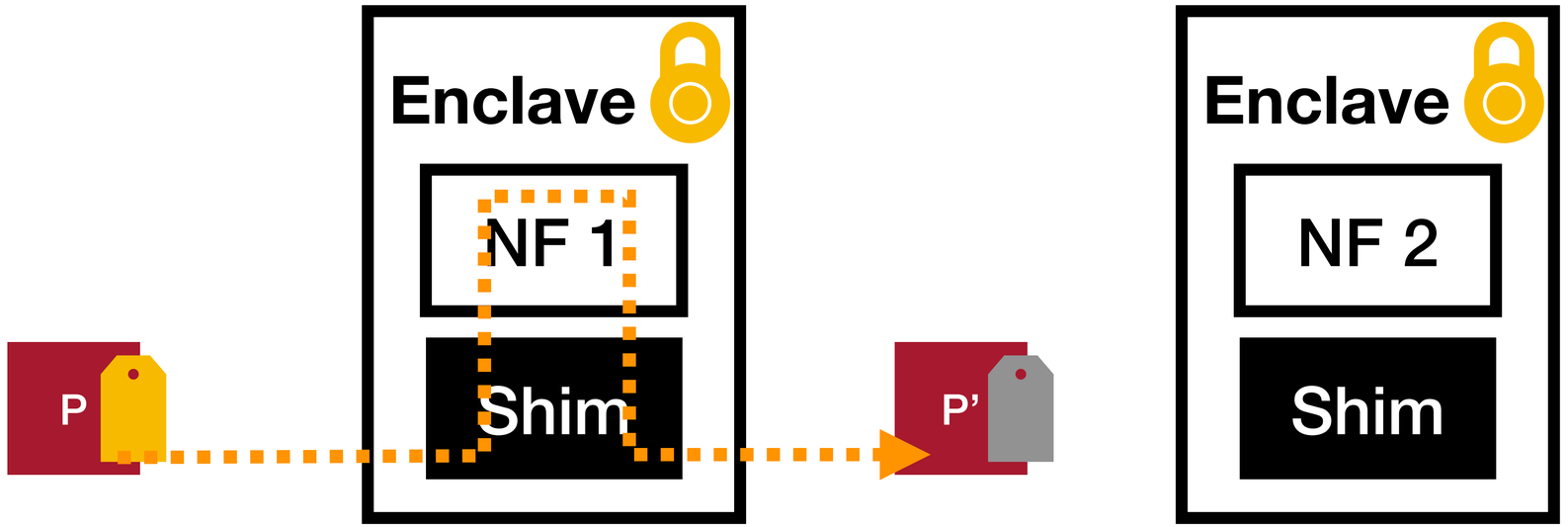
② NF Hop-by-Hop Updated Attestation



Audit Trailer

Packet ID	SRC NF	DST NF	Tag

② NF Hop-by-Hop Updated Attestation

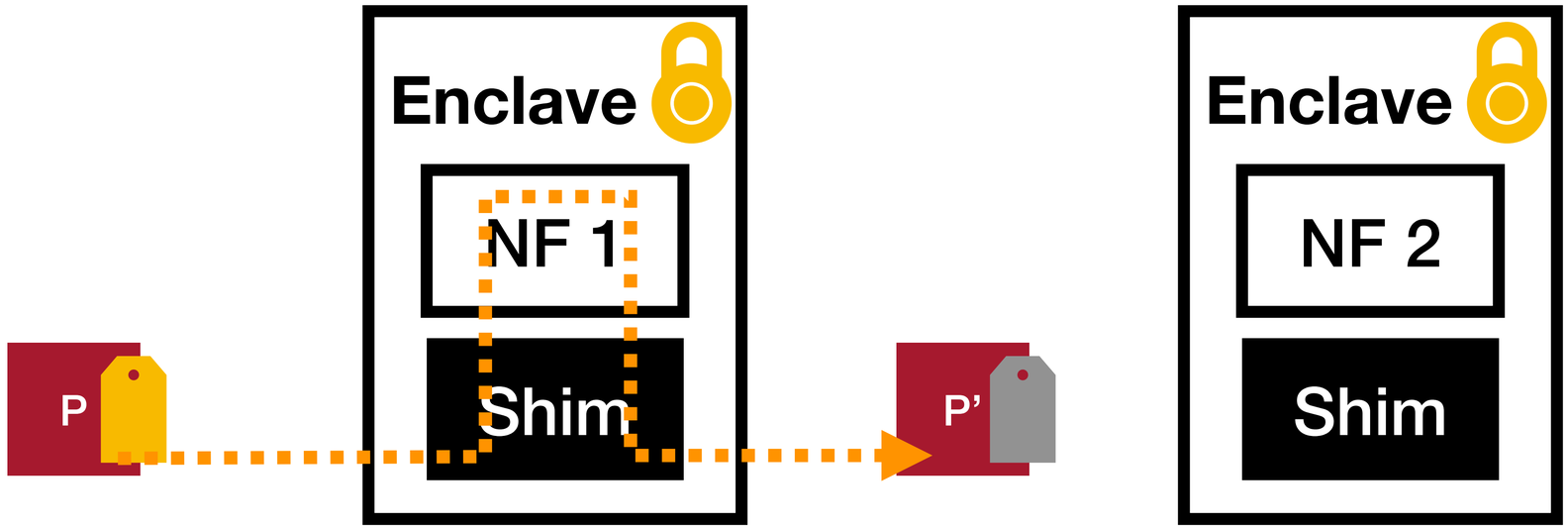


Audit Trailer

Packet ID	SRC NF	DST NF	Tag

Tag = GMAC(key, Packet | Packet ID | SRC NF | DST NF)

② NF Hop-by-Hop Updated Attestation



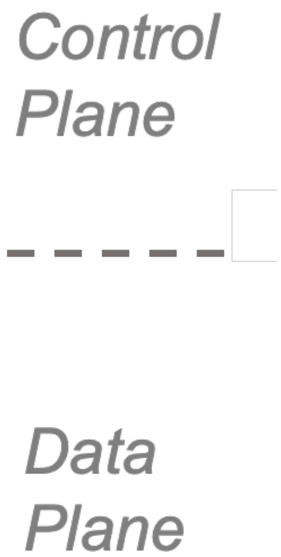
Audit Trailer

Packet ID	SRC NF	DST NF	Tag

Tag = GMAC(key, Packet | Packet ID | SRC NF | DST NF)

*AuditBox also supports **flow-level correctness** which detects packet duplication, reordering and drops (refer to paper for details)

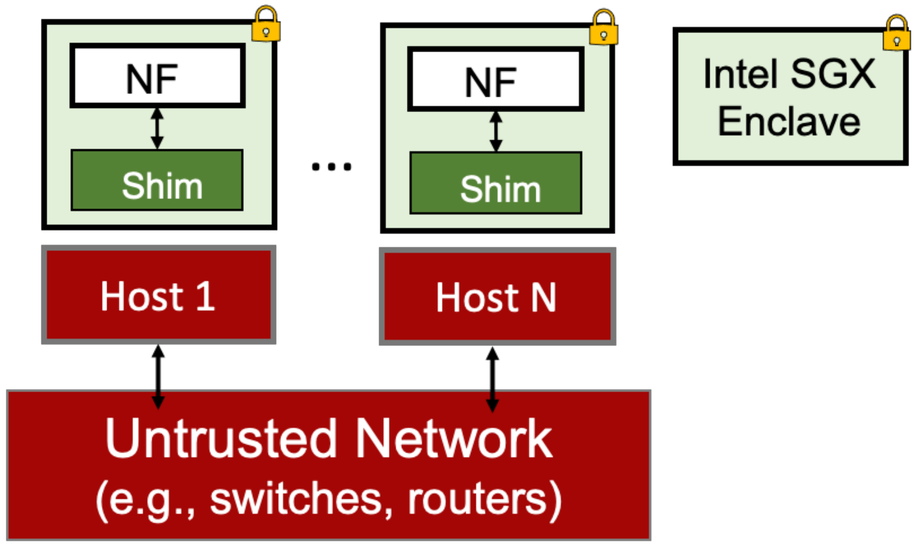
AuditBox Design Overview



AuditBox Design Overview

Control Plane

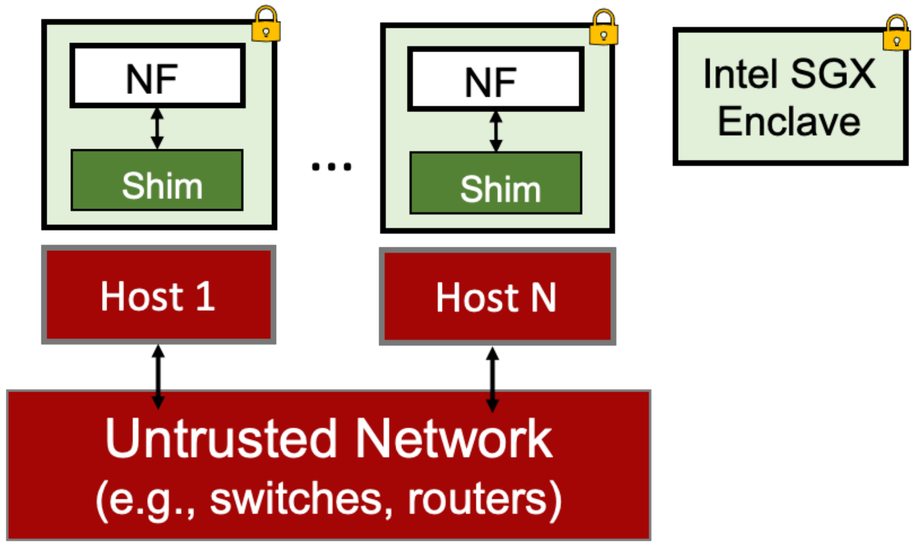
Data Plane



AuditBox Design Overview

Control Plane

Data Plane

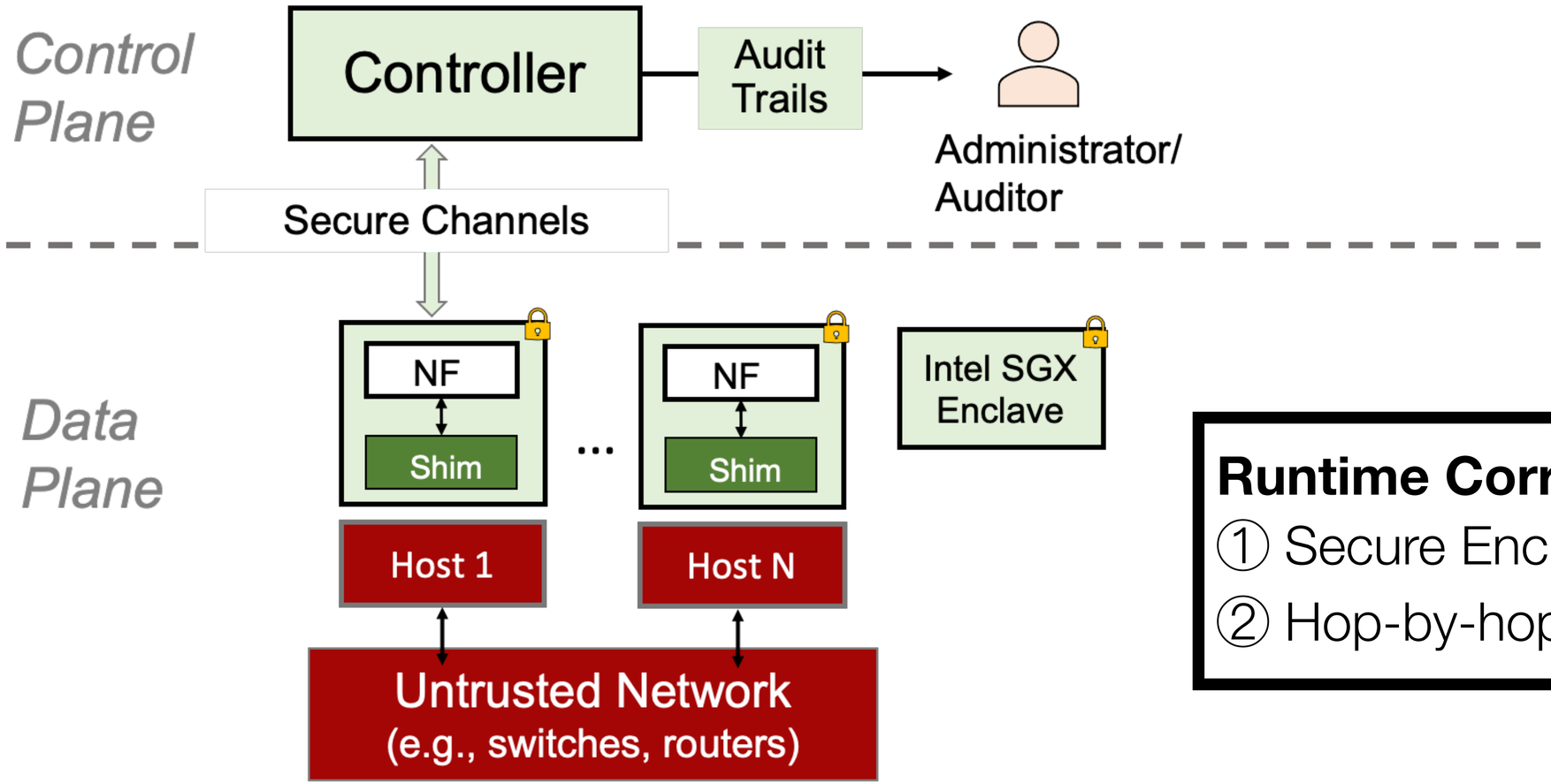


Runtime Correctness

① Secure Enclaves

② Hop-by-hop Verification Protocol

AuditBox Design Overview

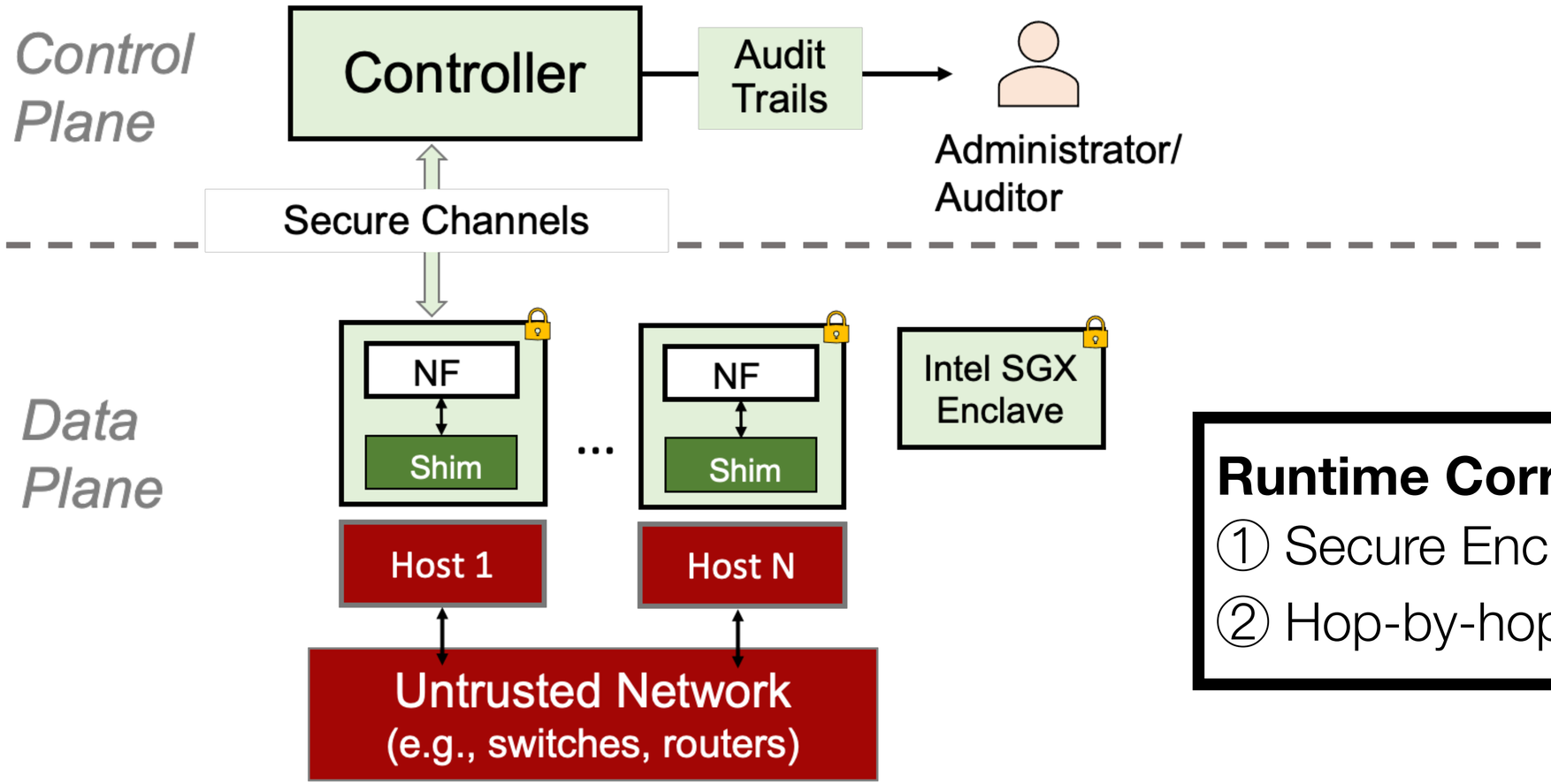


Runtime Correctness

① Secure Enclaves

② Hop-by-hop Verification Protocol

AuditBox Design Overview



Offline Auditability

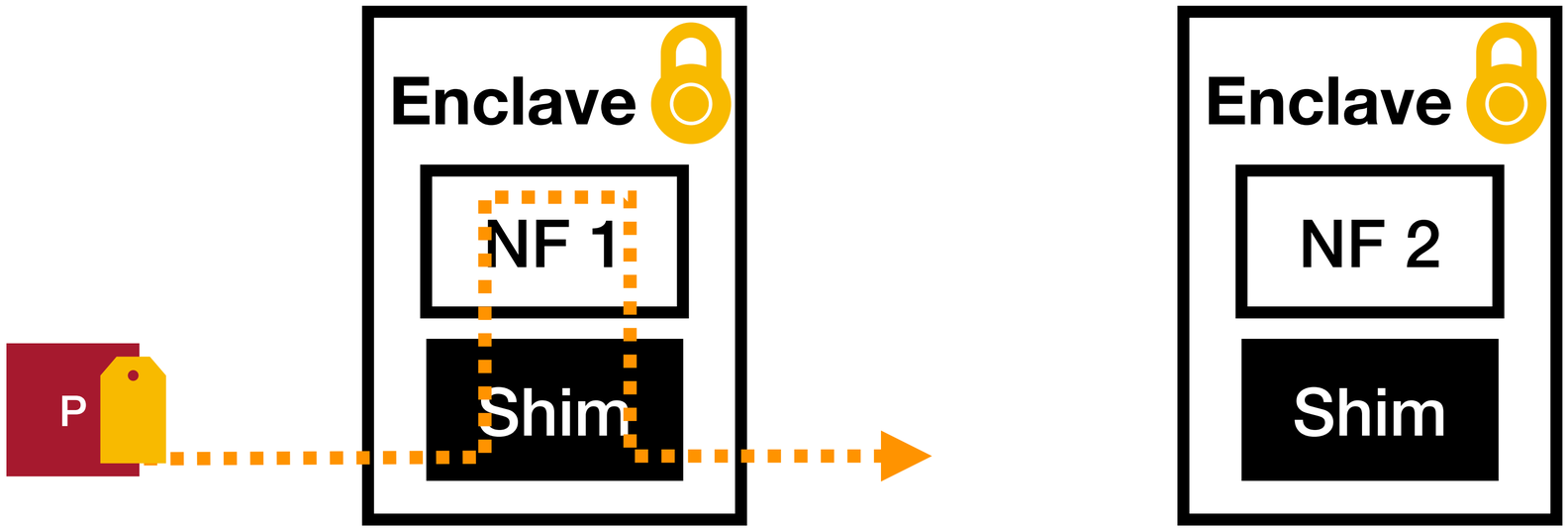
③ Secret Logging

Runtime Correctness

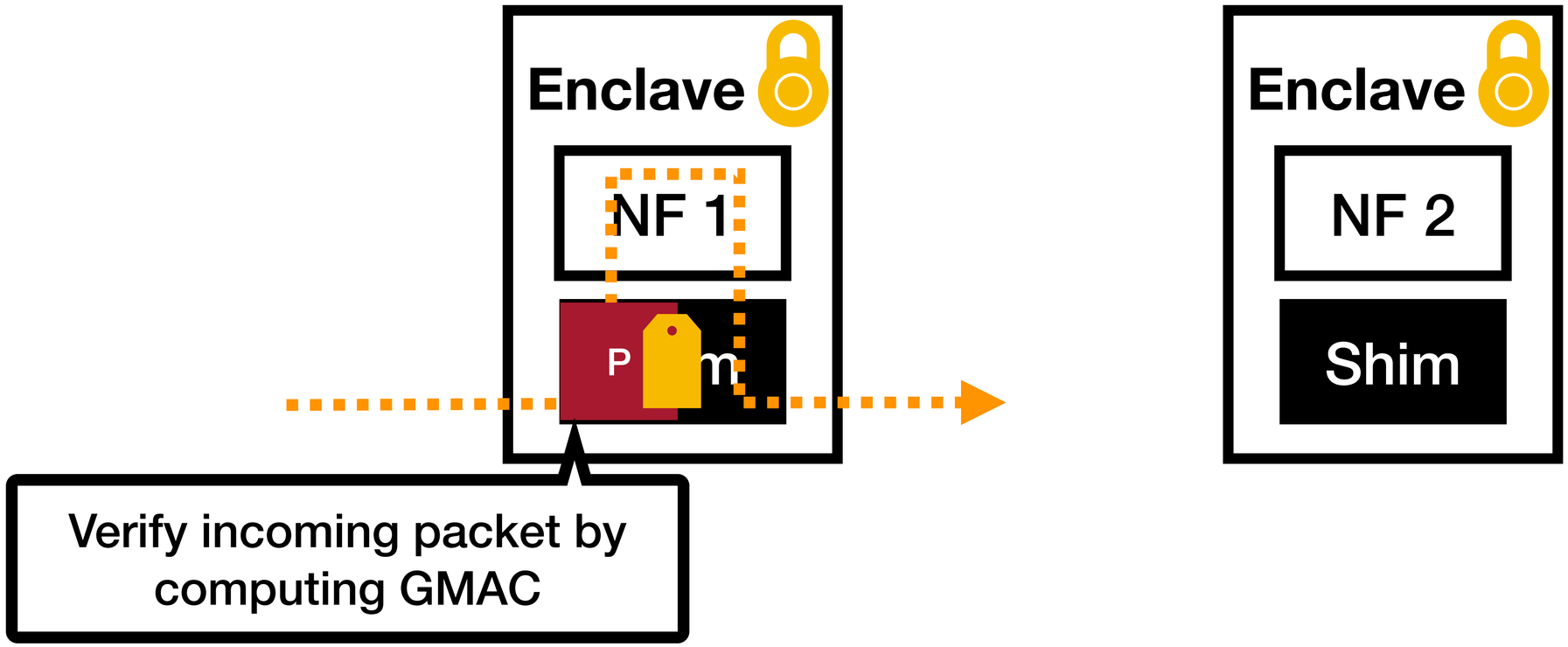
① Secure Enclaves

② Hop-by-hop Verification Protocol

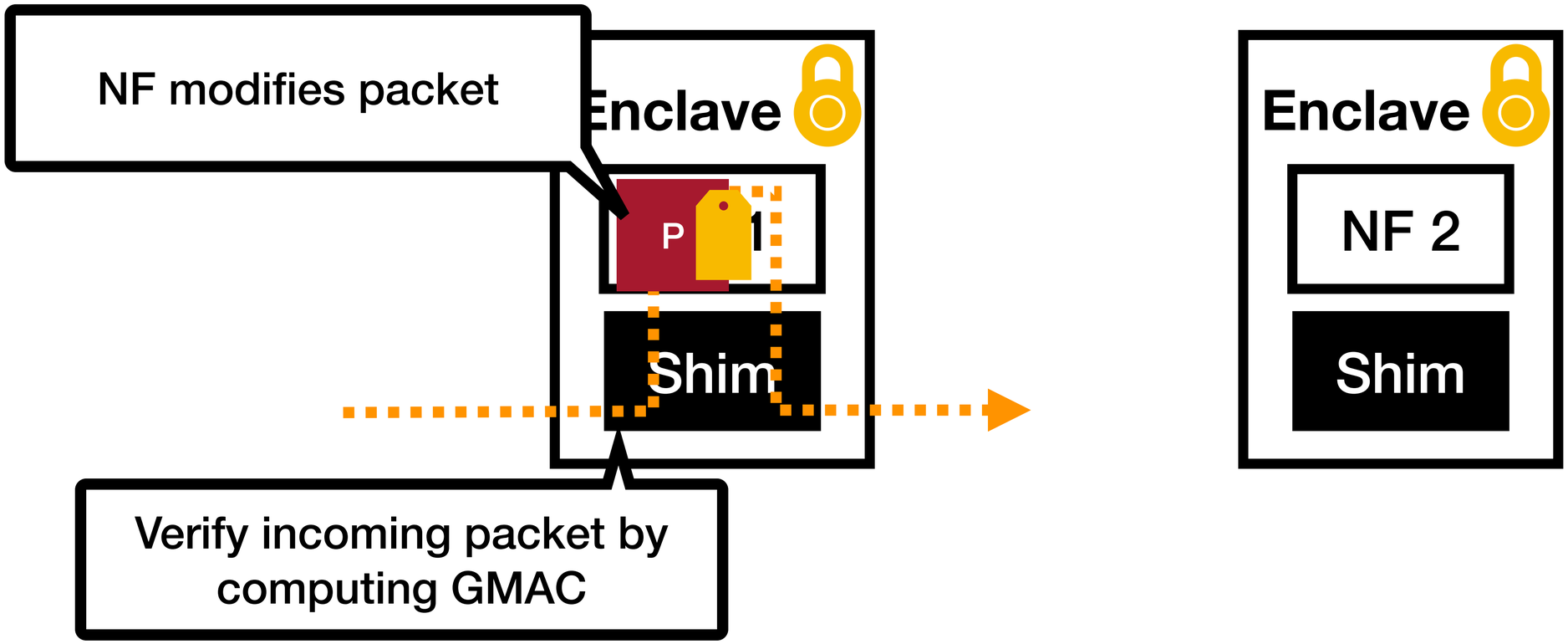
Potentially Crypotographically Expensive



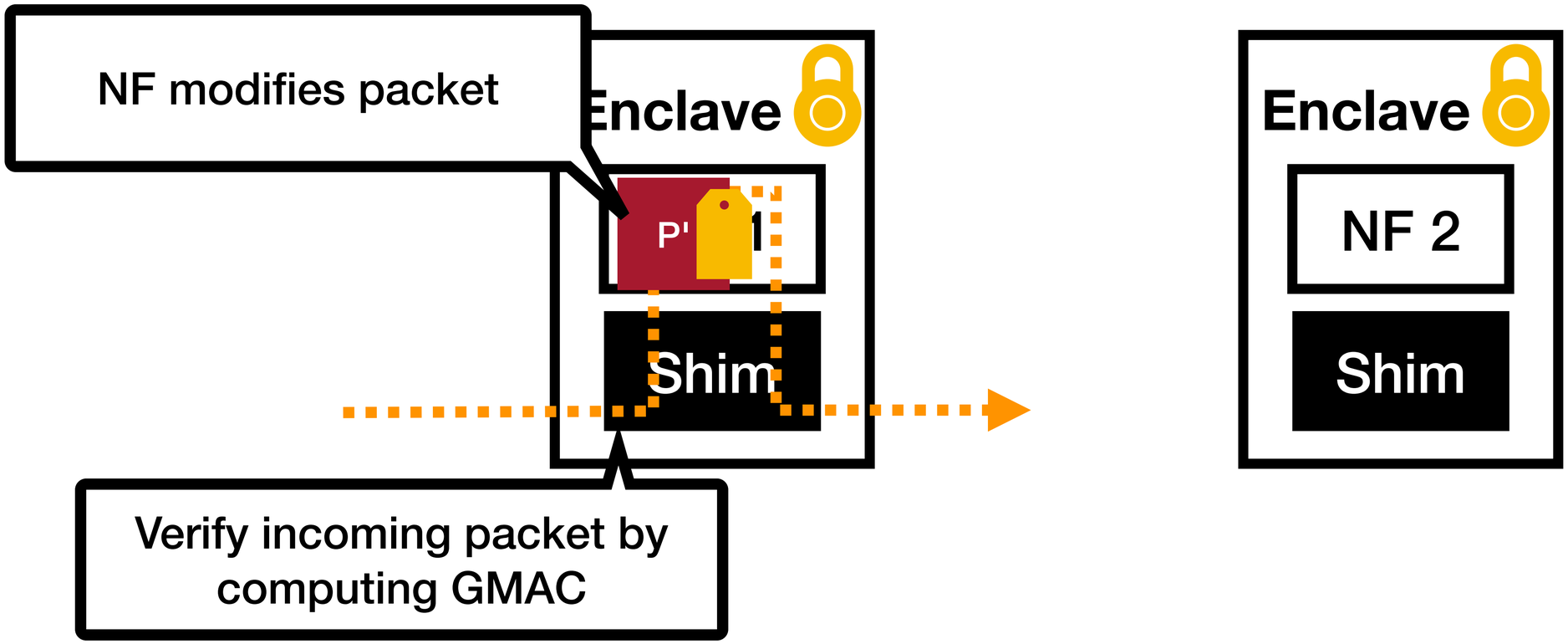
Potentially Crypotographically Expensive



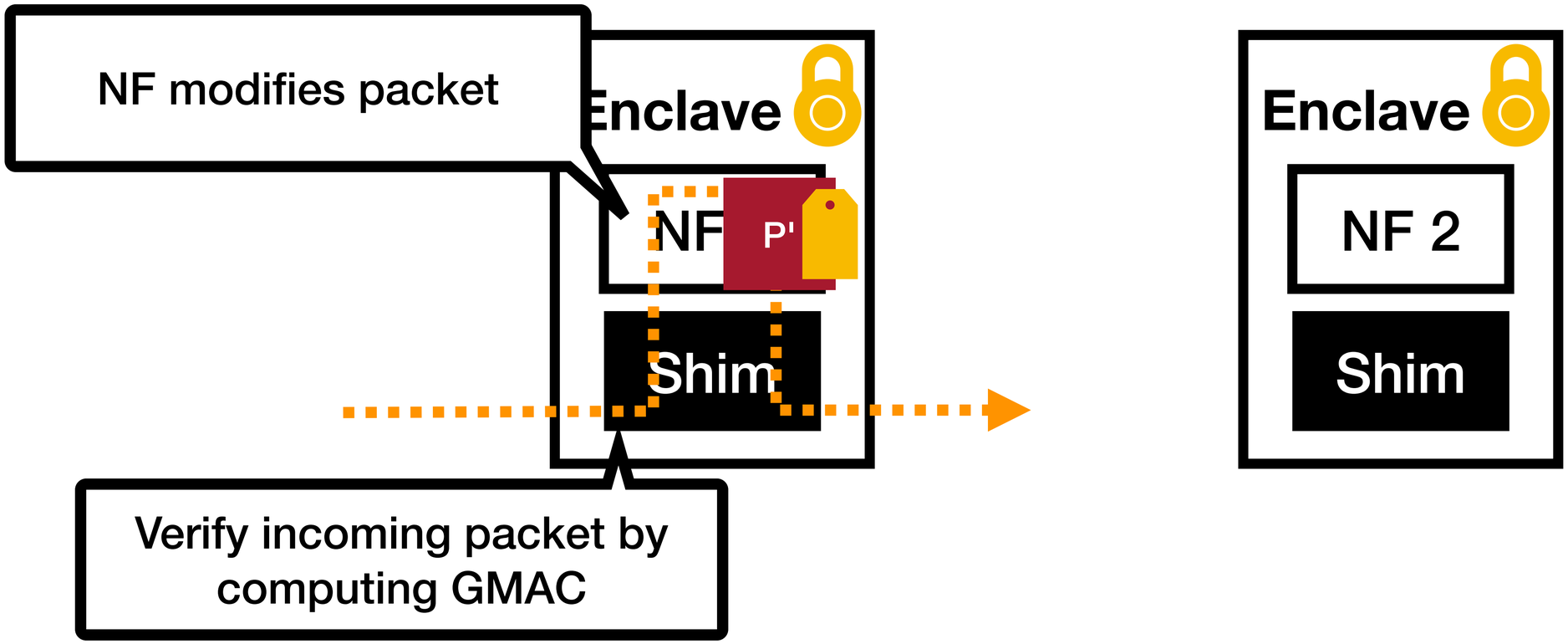
Potentially Crypotographically Expensive



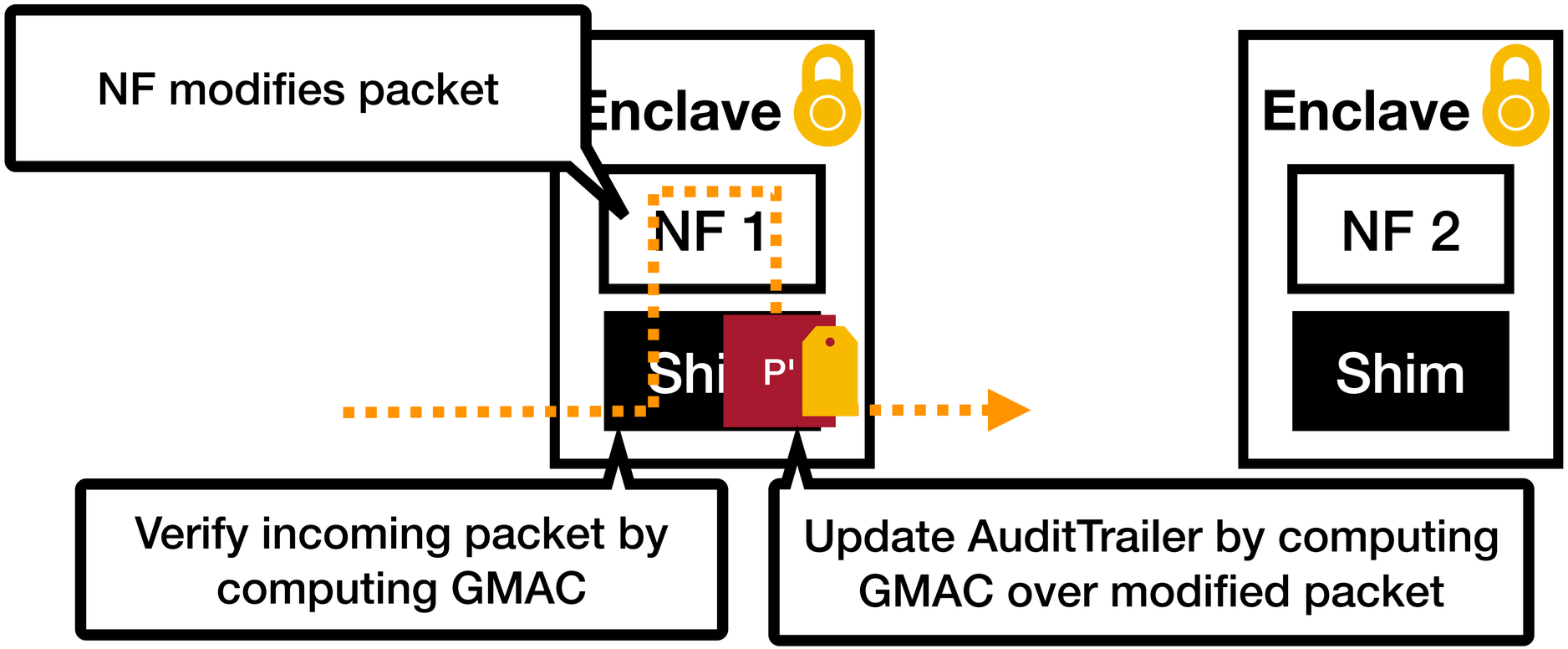
Potentially Crypotographically Expensive



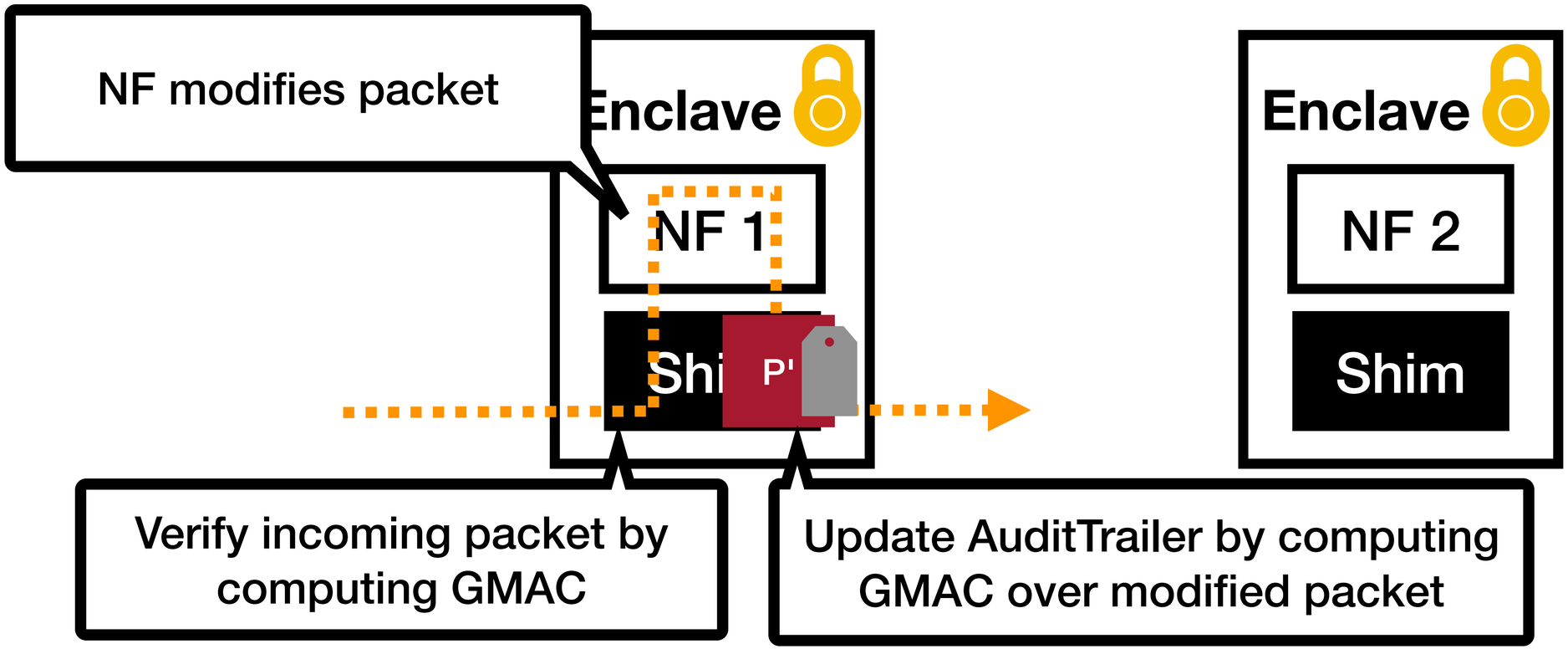
Potentially Crypotographically Expensive



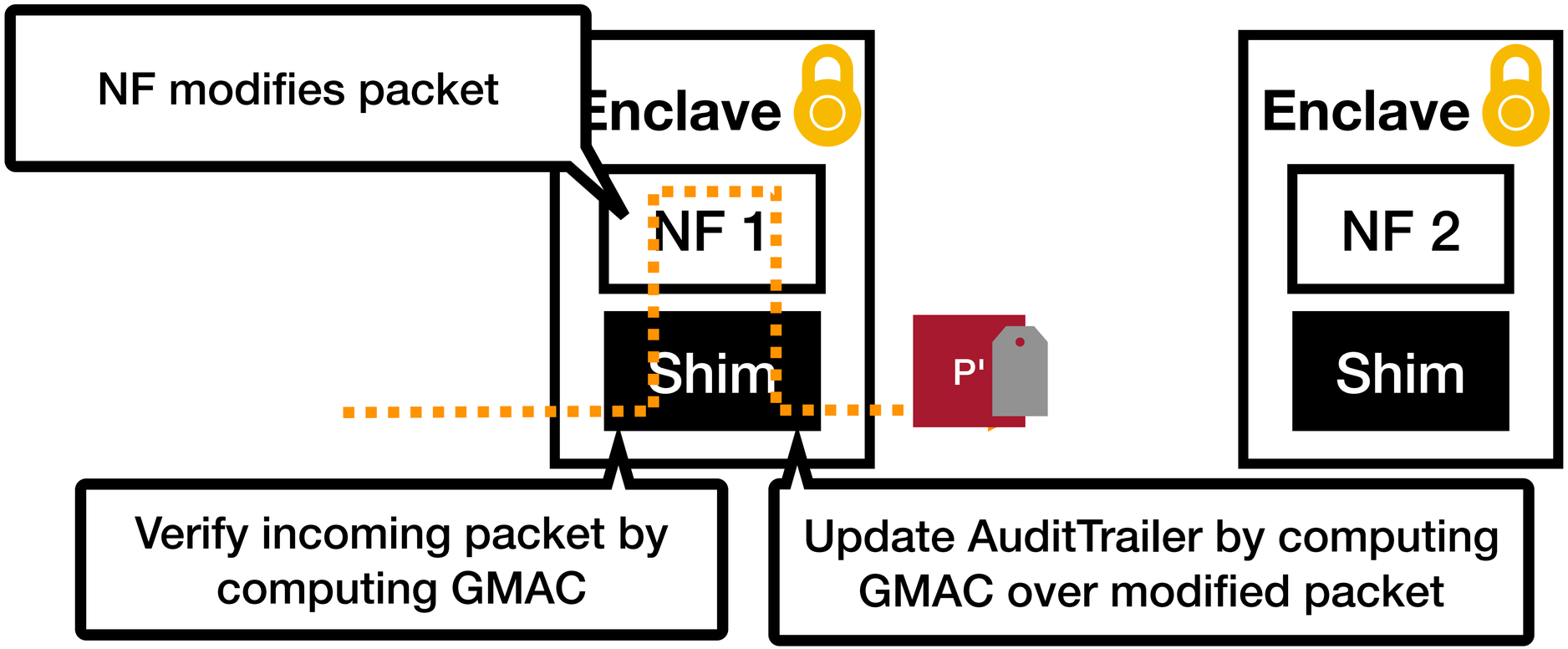
Potentially Crypotographically Expensive



Potentially Crypotographically Expensive



Potentially Crypotographically Expensive



- Asymmetric key at every hop
- 2 GMACs at every hop

④ Efficient Crypto Mechanisms

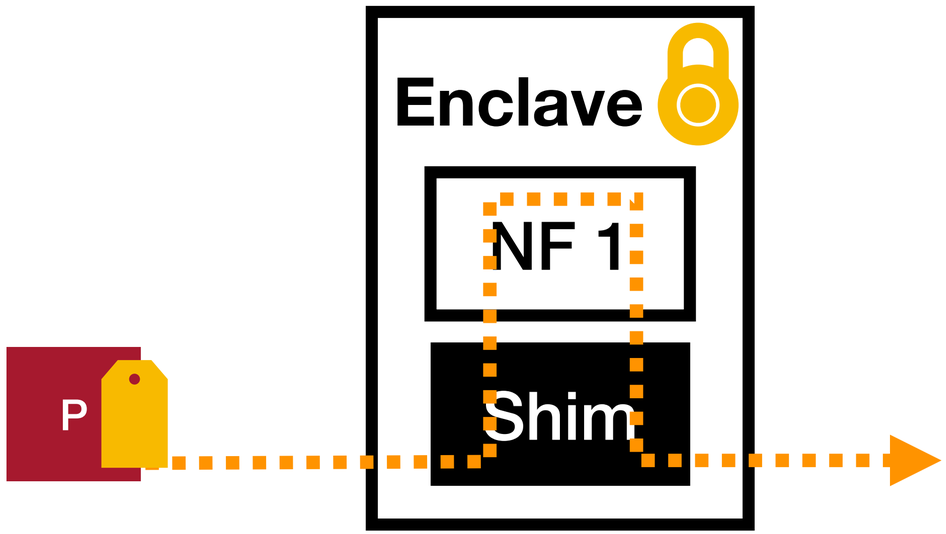
Audit Trailer

Packet ID	SRC NF	DST NF	Tag

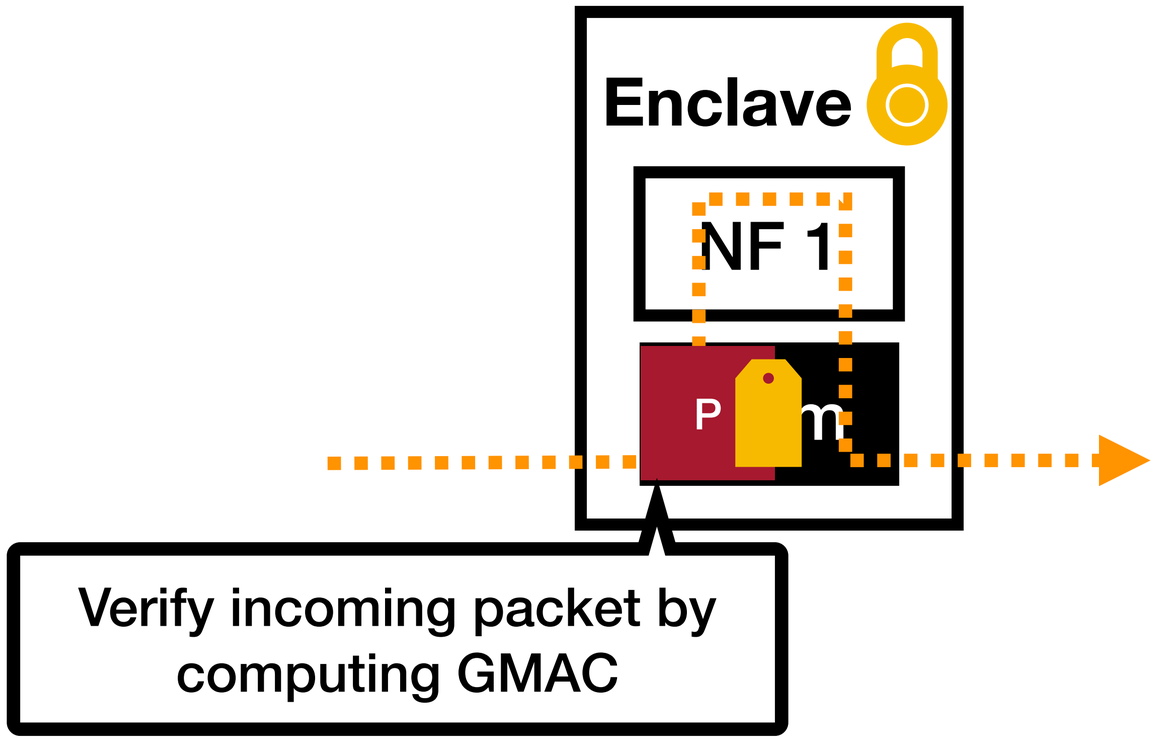
Tag = GMAC(**key**, Packet | Packet ID | SRC NF | DST NF)

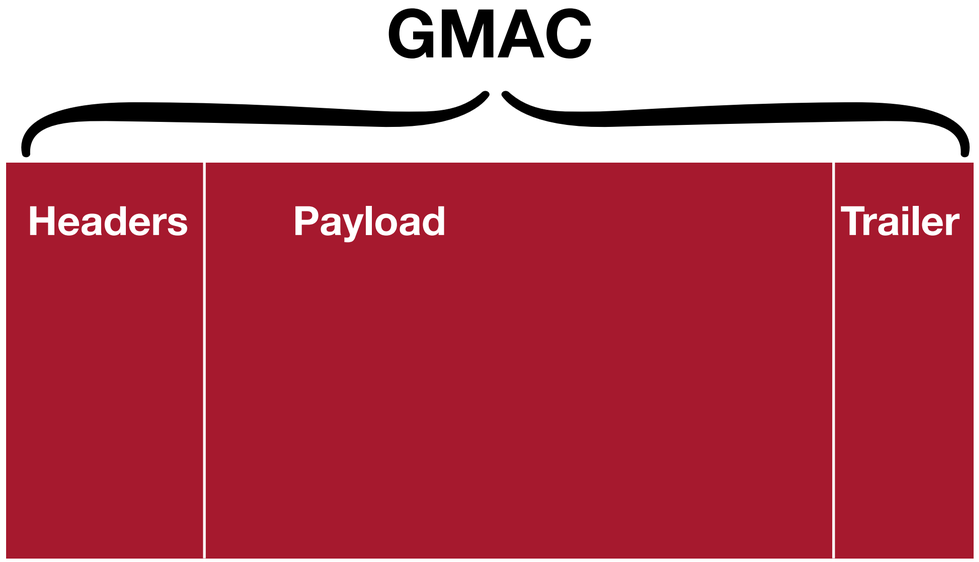
One symmetric key for all NFs in the same policy pipelet

④ Efficient Crypto Mechanisms

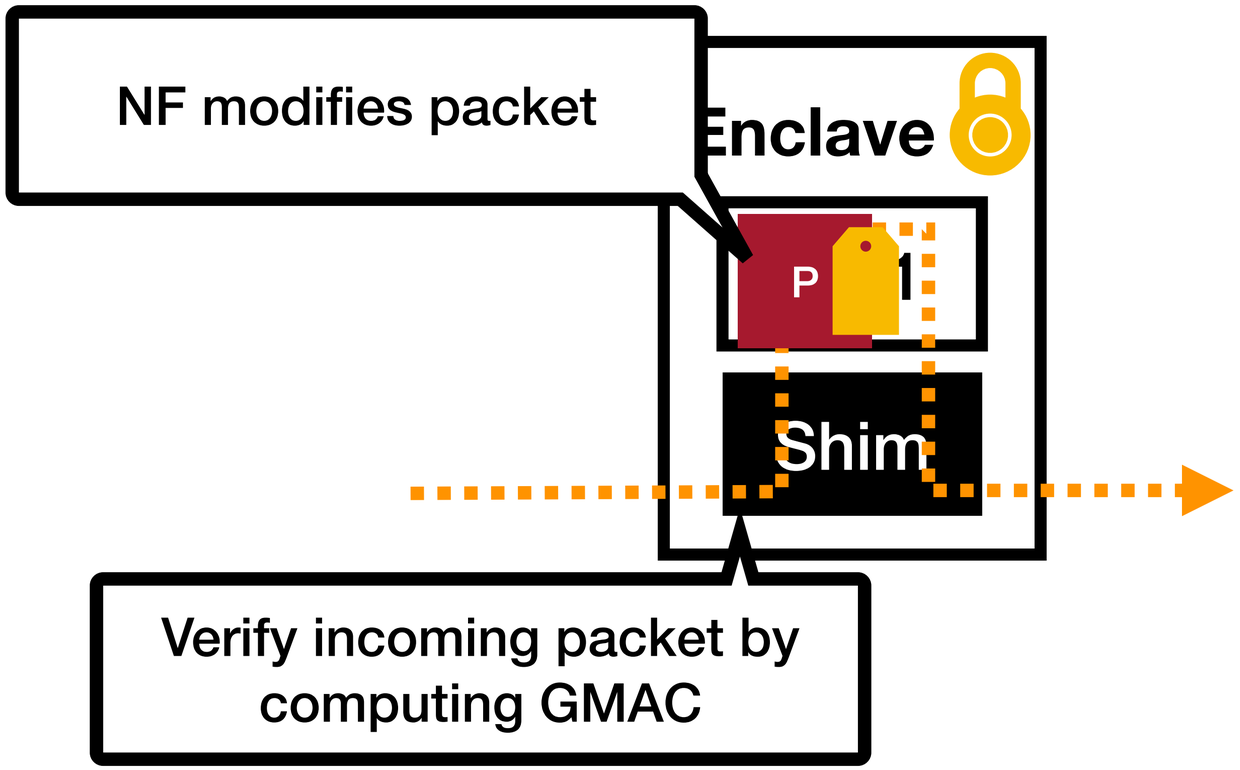


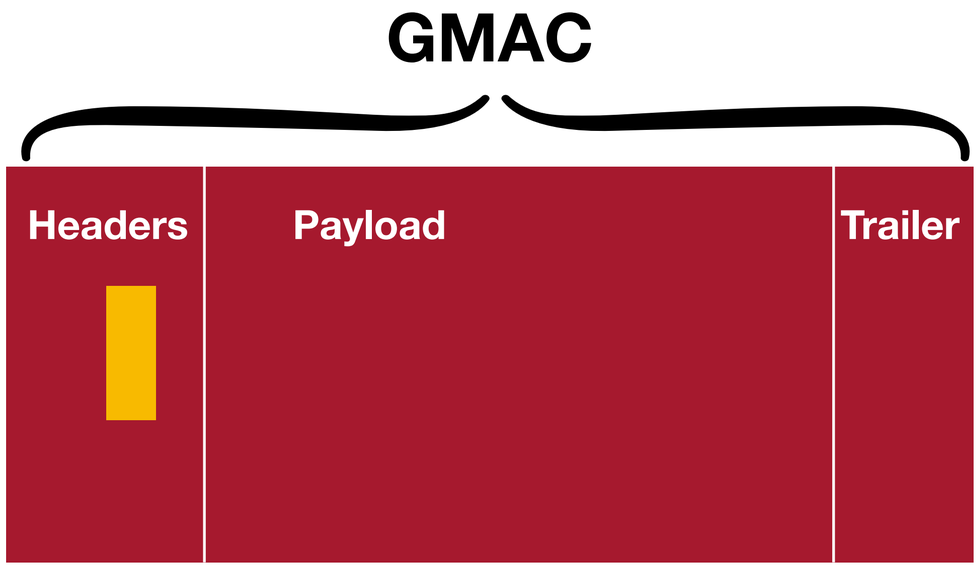
④ Efficient Crypto Mechanisms



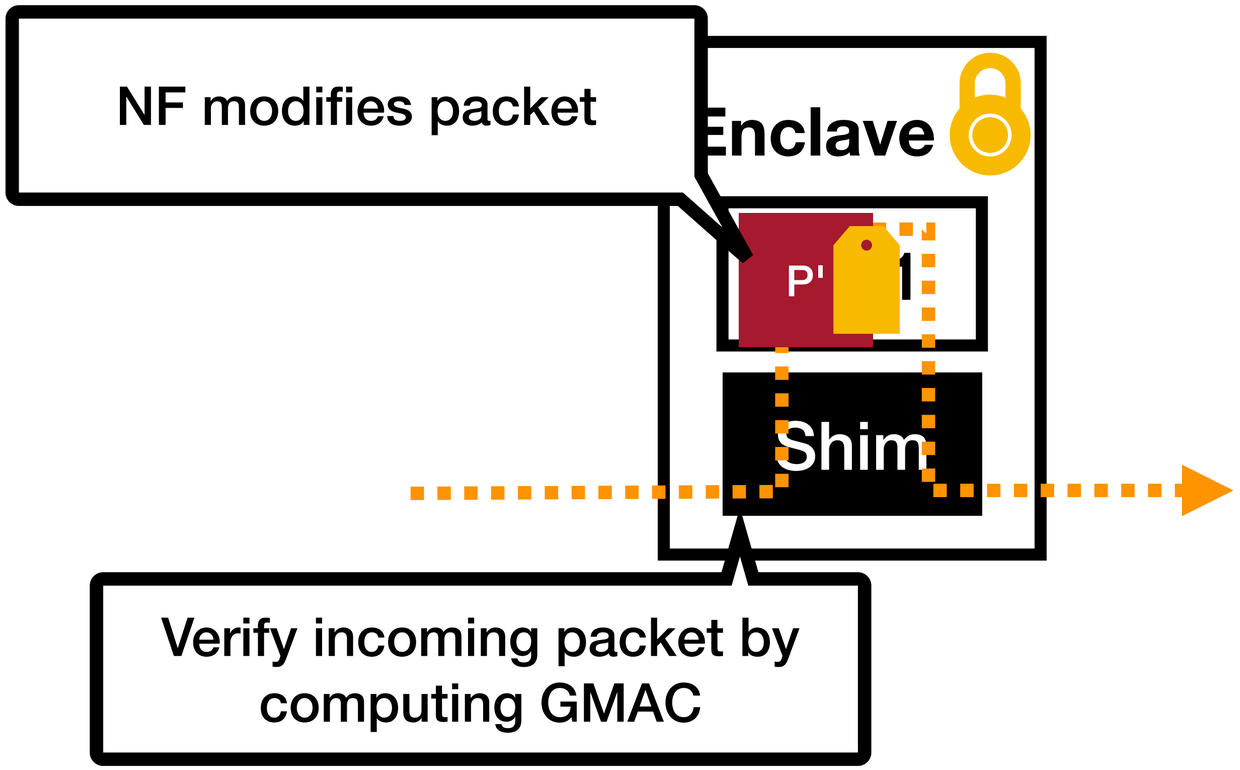


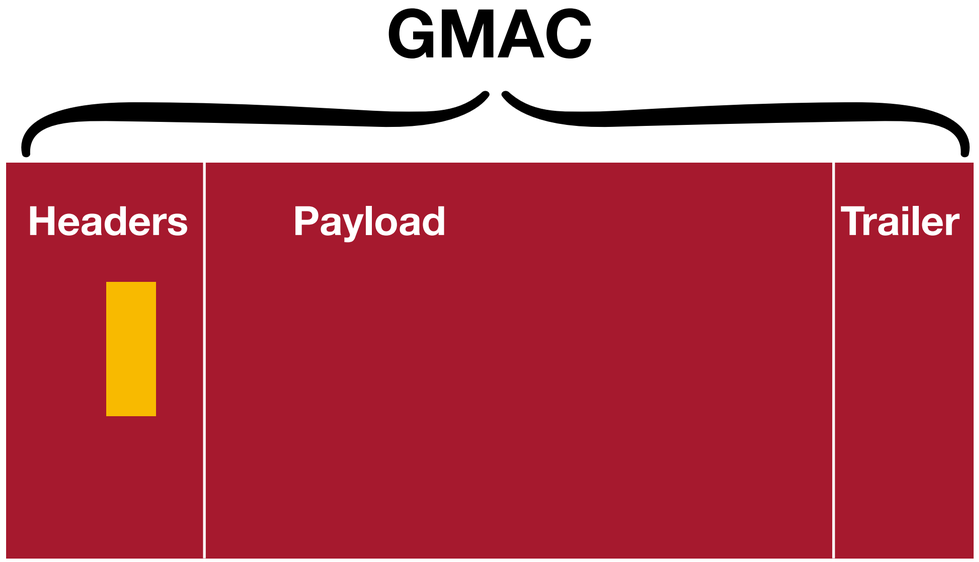
④ Efficient Crypto Mechanisms



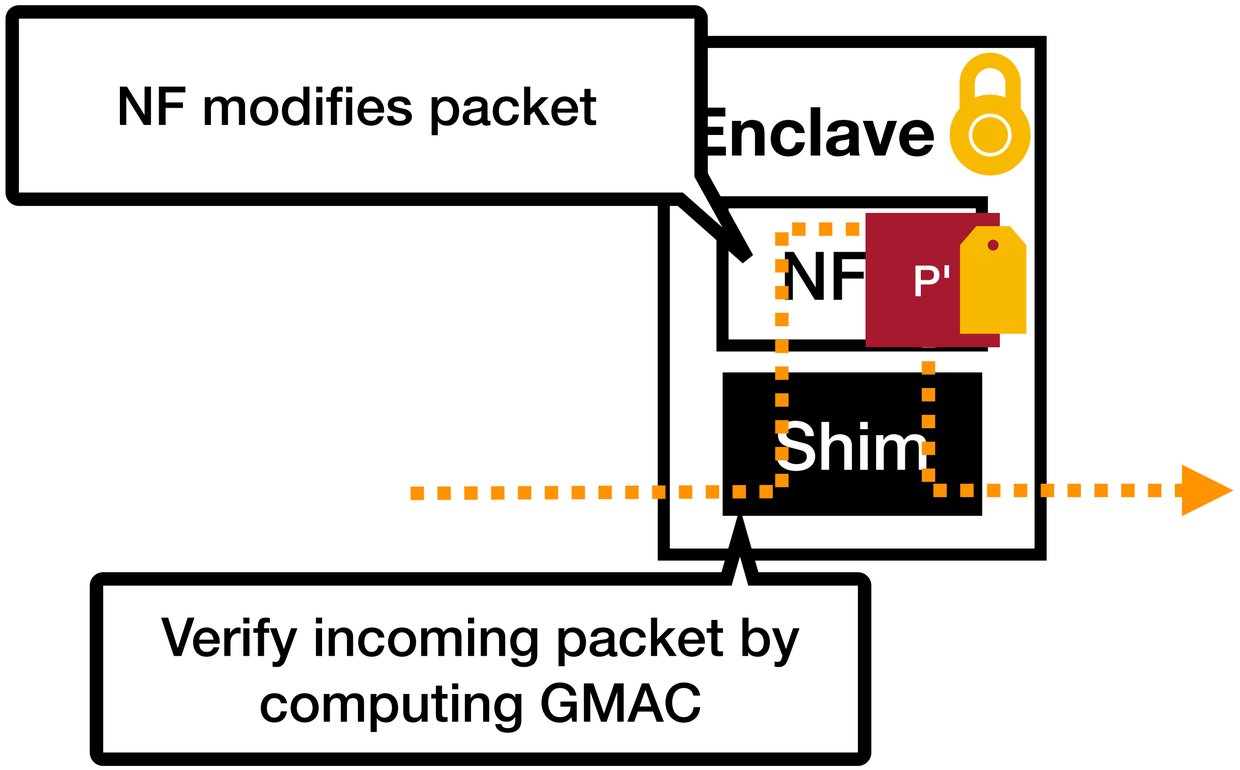


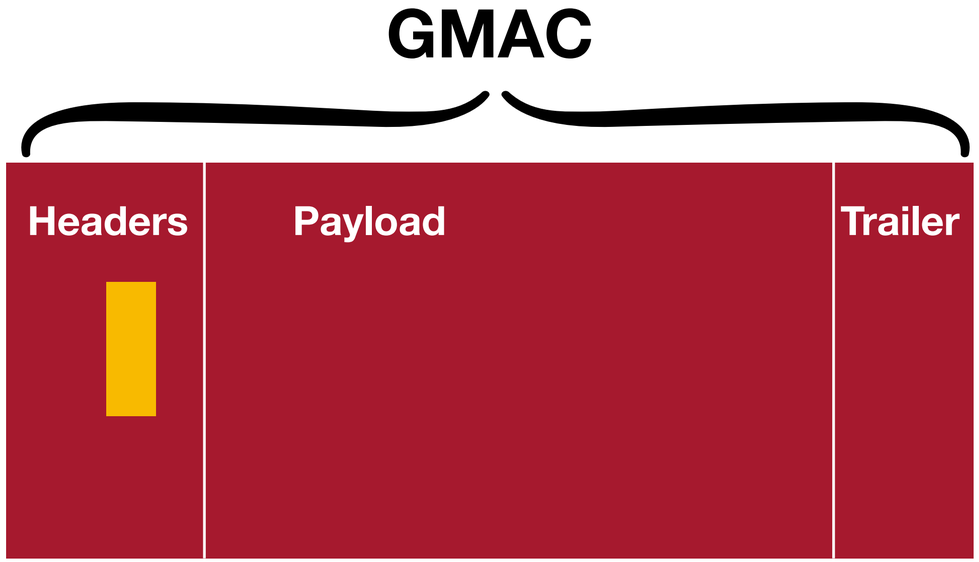
④ Efficient Crypto Mechanisms



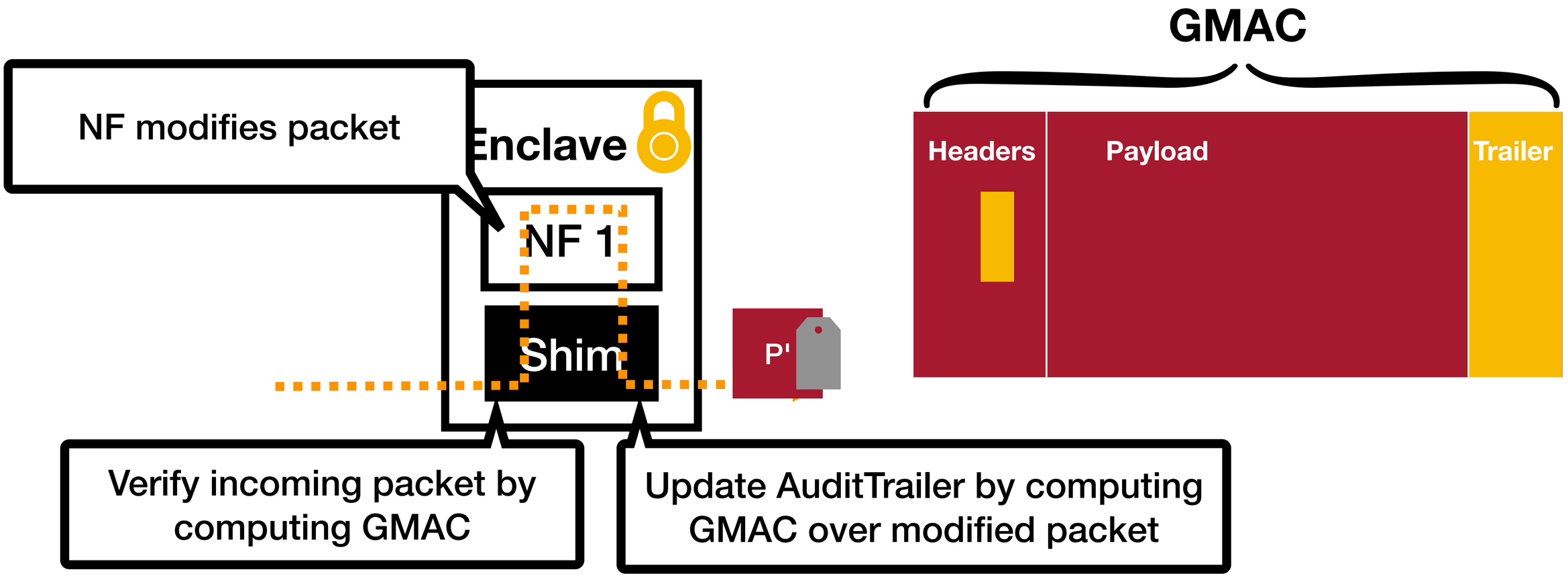


④ Efficient Crypto Mechanisms



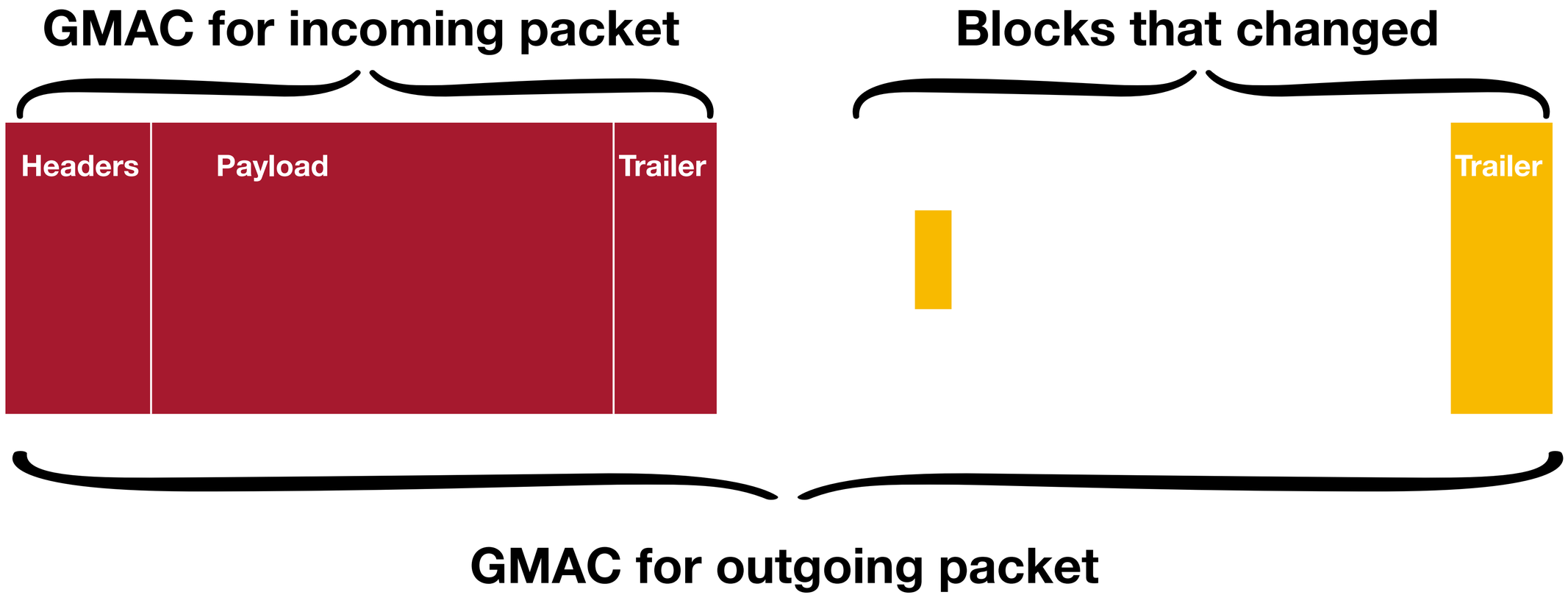


④ Efficient Crypto Mechanisms



④ Efficient Crypto Mechanisms

Updatable GMAC [1]: Reuse first GMAC when computing the second GMAC



[1] D. McGrew. Efficient authentication of large, dynamic data sets using Galois/counter mode (GCM). In Security in Storage Workshop. IEEE, 2005.

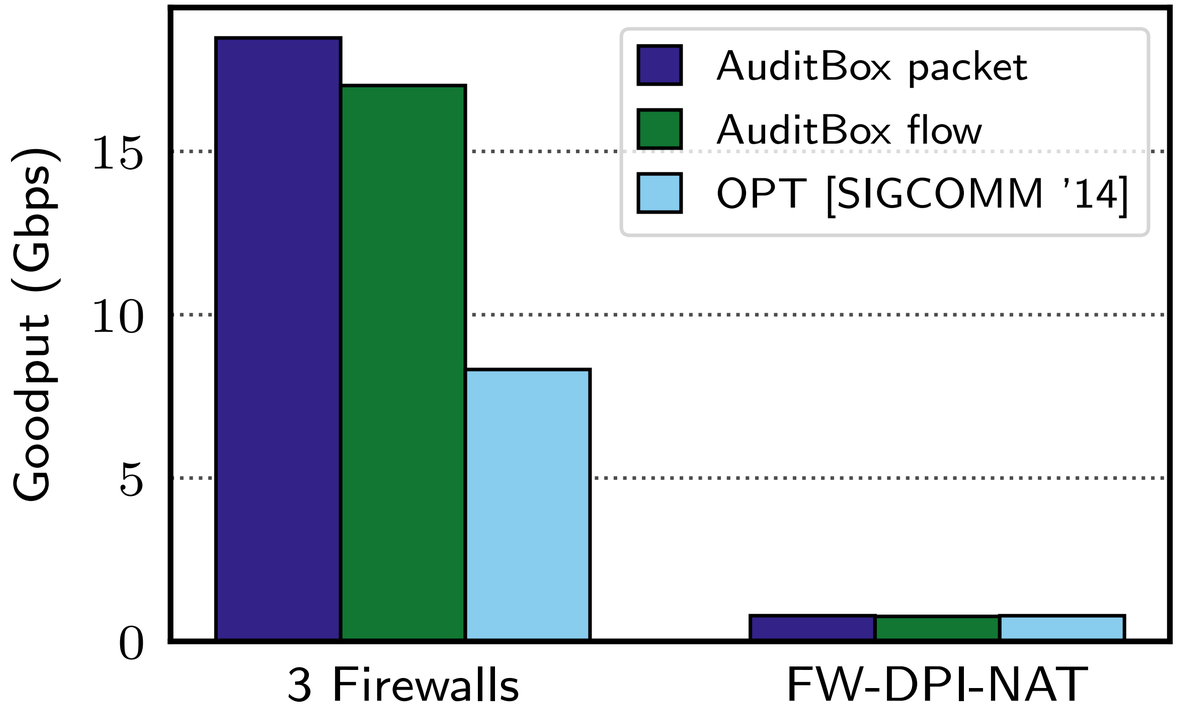
Evaluation

① **Proofs:** We provide security proofs that AuditBox can achieve both runtime correctness and offline auditability

② **Functionality Evaluation:** AuditBox correctly detects a broad class of policy violations

③ **Performance Evaluation:** AuditBox enables auditing for unmodified NFs with low overhead

Evaluation: NF Chain Goodput



Achieves 18 Gbps for a simple NF chain

Summary

AuditBox is the first NFV auditing system. It leverages **trusted execution environments** to provide:

- Runtime correctness
- Offline auditability
- While still achieving good performance

Don't Yank My Chain: Auditable NF Service Chaining

Guyue Liu, Hugo Sadok, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, Justine Sherry*

Carnegie Mellon University **Princeton University*

Contact: sadok@cmu.edu