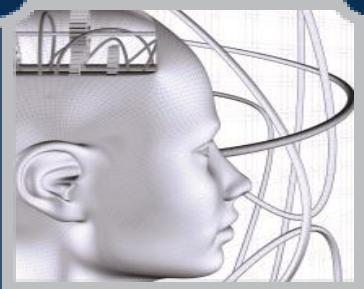
Design Considerations and Lessons Learned for Building Cyber Deception Systems

October 30, 2017

Gregory Briskin, Jason Li
Intelligent Automation, Inc. (IAI)

Cyber Deception and Defense Workshop
ACM CCS 2017
The 24th ACM Conference on Computer and Communications Security



Intelligent Automation, Inc.
15400 Calhoun Drive, Suite 190
Rockville, MD 20855

Introduction and Scope

❑ Cyber Deception for Protection

- Improve a defensive posture, protect cyber-assets and infrastructure of a given mission, in order to waste the attacker's resources while permitting time to organize a better defense

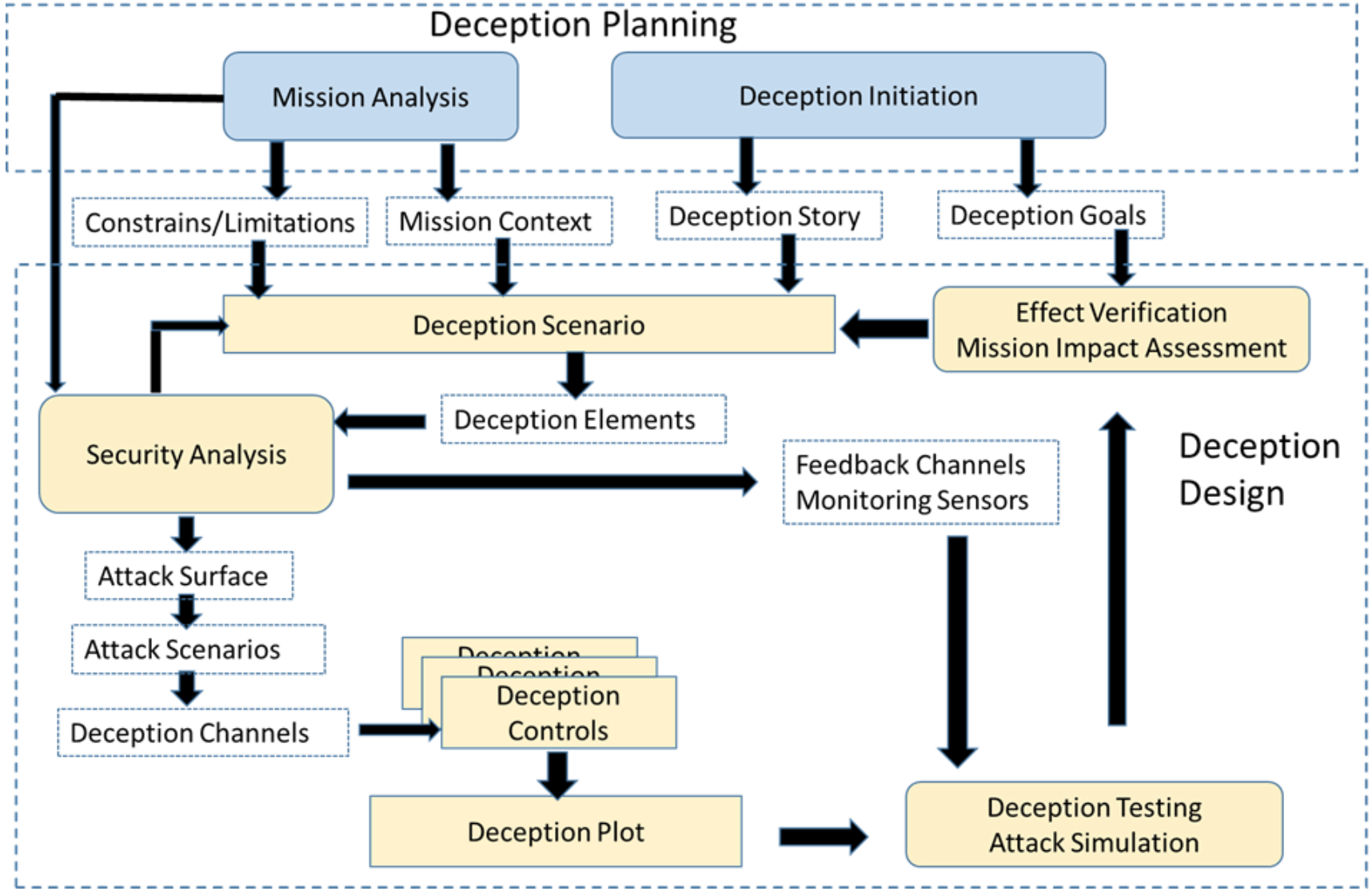
❑ Deception Design Considerations and Challenges

❑ Building Deception Plot to Address the Challenges

❑ Trying Different Implementation Platforms

❑ Lessons Learned and Future Work

Deception Design Workflow



Goals: Network-based Deception Against Reconnaissance

❑ Spans multiple Phases of Cyber Kill Chains

- External and Internal Reconnaissance (early vs. later attack phases)

❑ Active Reconnaissance

- Network scanning and topology mapping
- Host discovery, OS identification, service enumeration, configuration harvesting

❑ Passive Reconnaissance

- Monitoring and capturing network traffic inside the network

❑ Methods

- Direct observation of the target (e.g., monitoring network activity),
- Collecting and collaborating the evidence about the target (e.g., direct and indirect probing)
- Learning about the target from neighboring network objects, resource repositories, etc.

Deception Goals

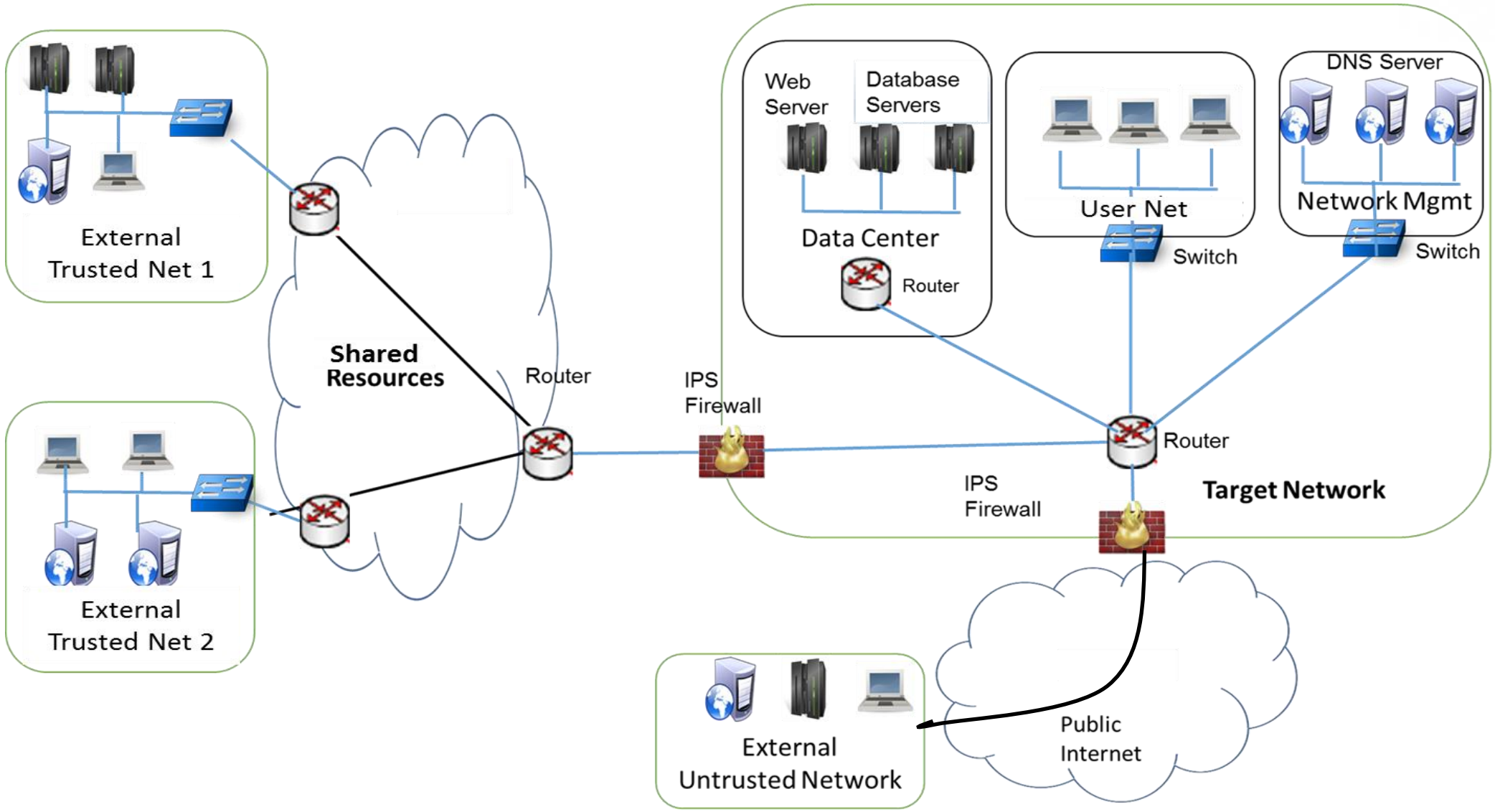
❑ Objectives

- Keep attackers stuck in the reconnaissance phase or forced to move on to the next stage with imperfect intelligence
- Waste the attacker's resources; increase the attackers' work factor
- Impede, deflect attention and mitigate potential exposure

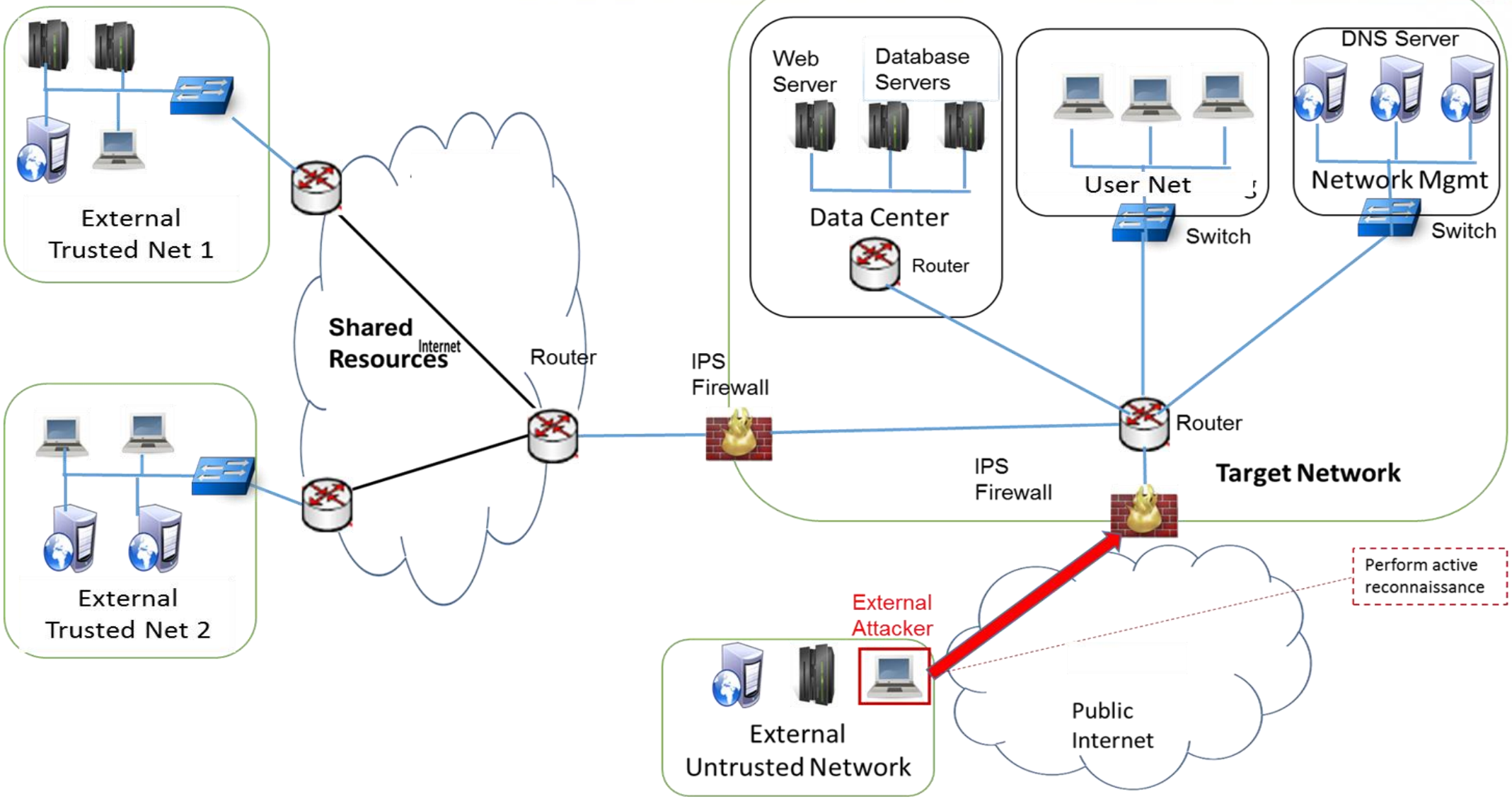
❑ Approach

- Hide the existence and/or the nature of shielded systems
- Create uncertainty, confusion, and complexity for the attackers
- Create noise around valuable information to alter adversary perception of its importance
- Monitor and manipulate adversarial reconnaissance process
- "The adversary should be able to verify the **veracity** of the deception story"

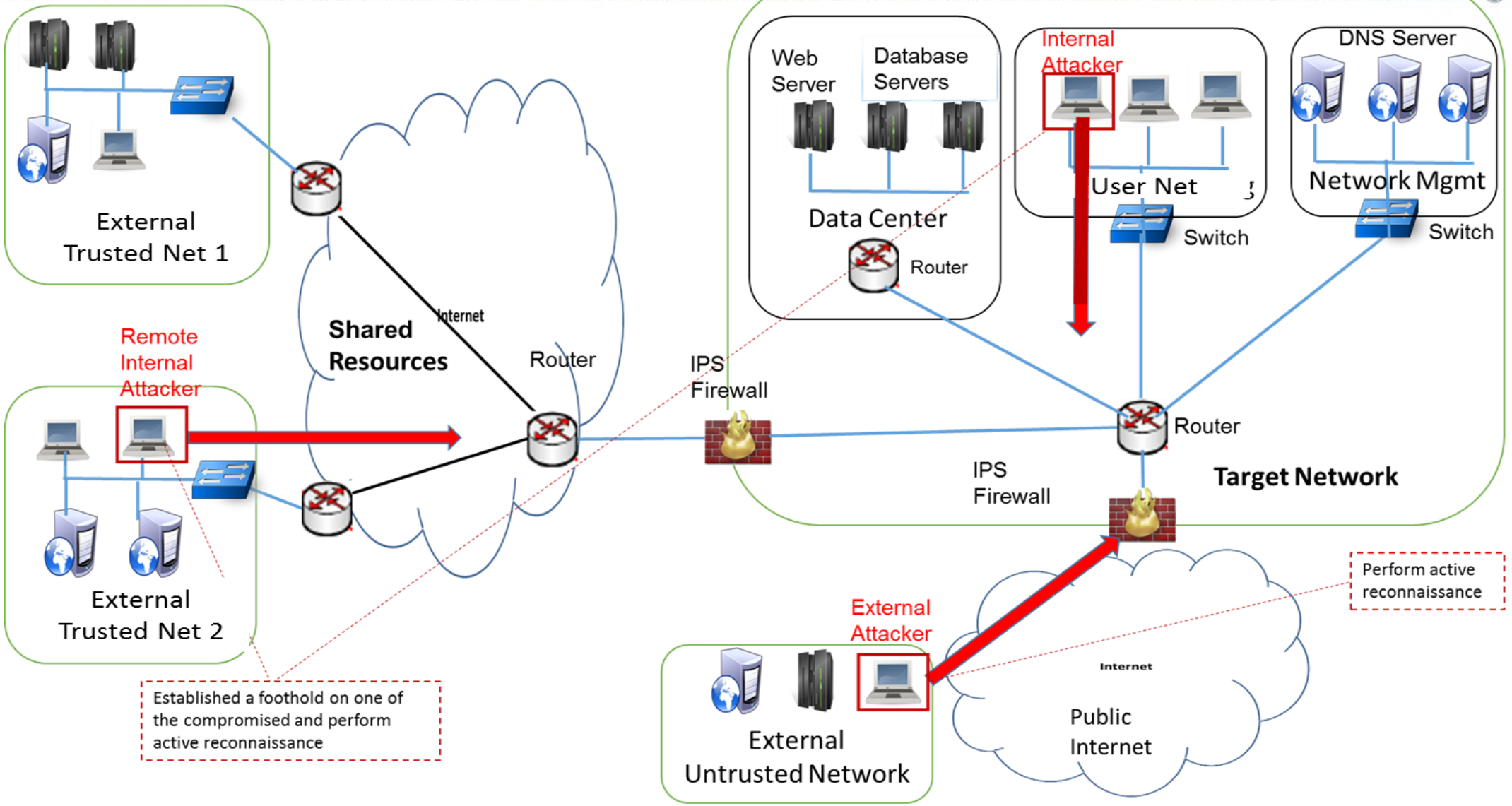
Context: Enterprise Network Environment



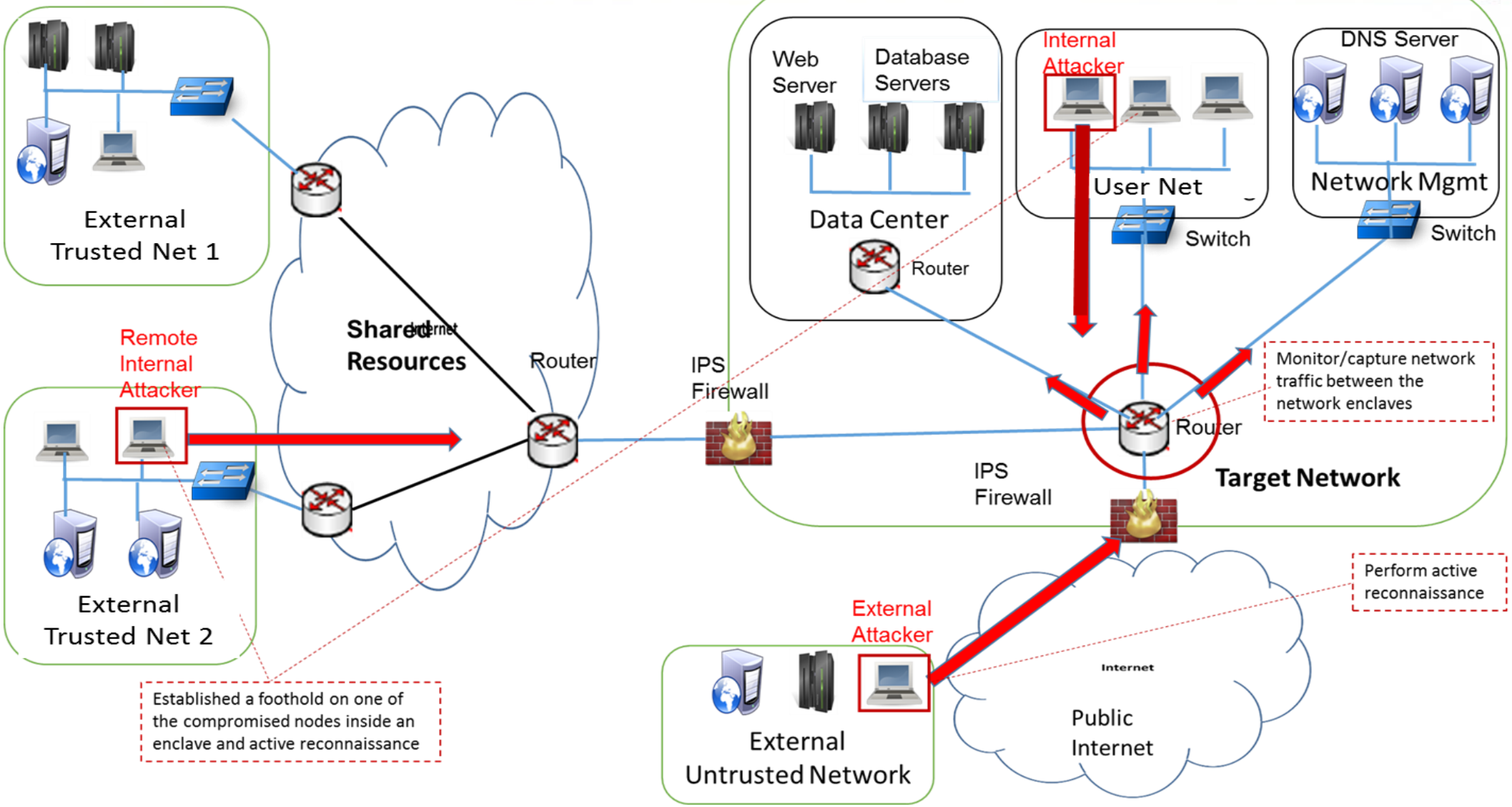
Attack Scenarios: External and Internal Network Reconnaissance



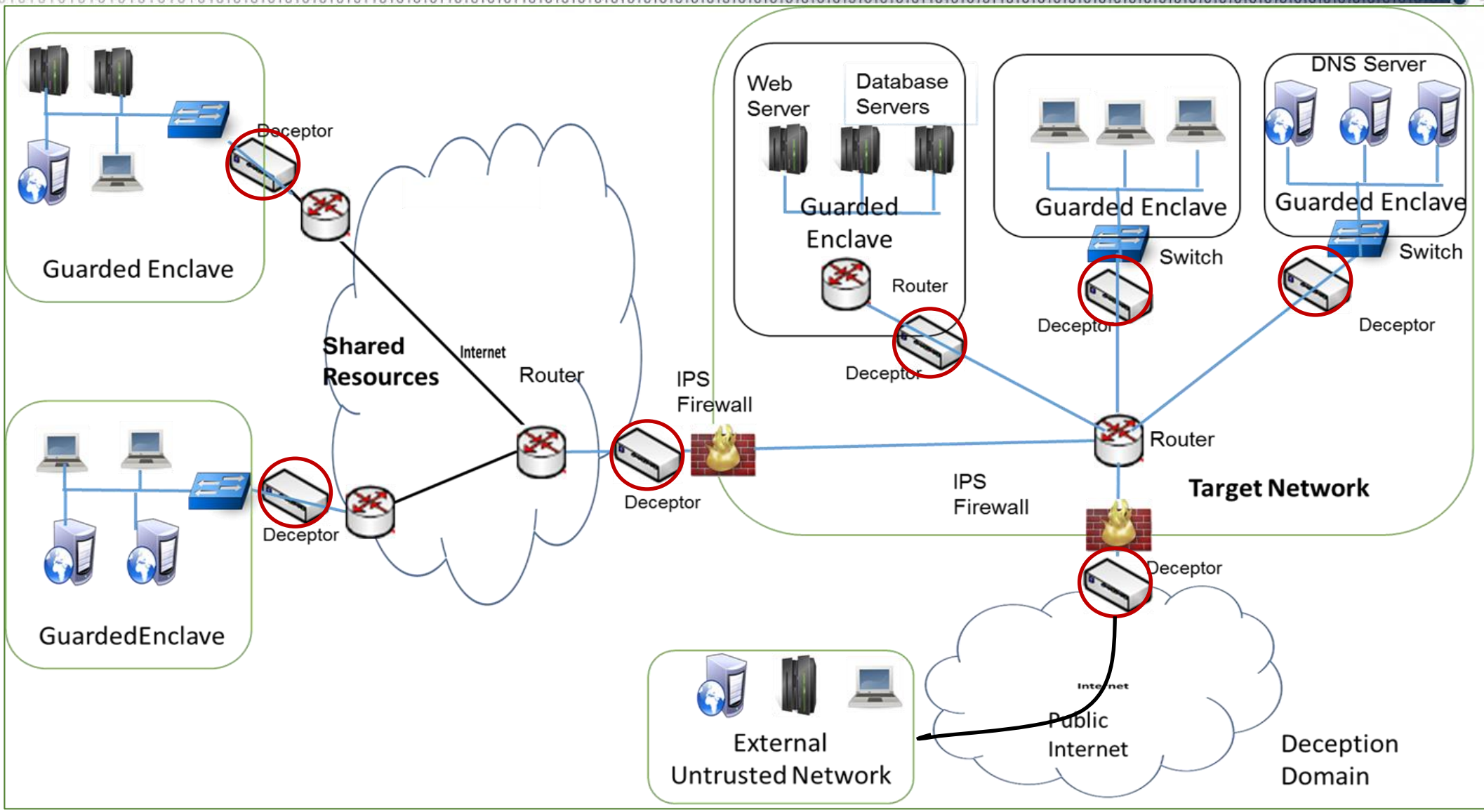
Attack Scenarios: External and Internal Network Reconnaissance



Attack Scenarios: External and Internal Network Reconnaissance



Building Deception Channels



Deception Scenario: Properties

- **Depth -** deception methods must transcend different network protocols and OSI layers, host and networking boundaries
- **Consistency** - consistent or intentionally inconsistent information about a given element of deception
  - **Variety** – different indirect response information is given back to the attacker for probing techniques of different level of sophistication
  - **Timing** – forming perception of static or transient environment
  - **Coverage** of multiple cyber-kill chain phases
  - Multiplicity of **topological viewpoints**
- **Sustainability and duration** – deception life span
- Hardware and software platform support
- Attacker's work factor. Deception effects.

Selected Deception Elements

❑ Network Topology Falsification

- Hiding existing and presenting fictitious nodes/hosts, subnets and network paths
- Did not involve creating an actual or virtualized honeypots/nets

❑ Host Discovery Falsification

- Manipulating information about TCP/UDP ports available on real or fictitious hosts

❑ OS and Service Falsification

- TCP/IP-based OS identification deception
- Service banner modification

❑ Firewalking Deception

- Misinformation about ACLs, rulesets and capabilities of a targeted firewall

Deception Scenario: Challenges

- **Dependency on cyber-attack detection and attacker's profiling**
  - Determines triggers of deception scenarios
  - There could be false positives
  - Attacks could be stealthy, "smoke screens"
- **Coexistence / Interoperability with cyber defense controls**
- **Effectiveness of deployed deception**
  - Verifiability of deception story
  - Deception longevity and sustainability
  - Deception devices are subjects of attacks
- **From Localized Deception to Enterprise-wide Deception Scenarios**

Deception Plot: Overcoming the Challenges

- **Dependency on cyber-attack detection and attacker's profiling**
  - Determines triggers of deception scenarios
  - There could be false positives
  - Attackers could be stealth
- **Coexistence / Interoperability with cyber defense controls**
- **Effectiveness of deployed deception**
  - Verifiability of deception story
  - Deception longevity and sustainability
  - Deception devices are subjects of attacks
- **From Localized Deception to Enterprise-wide Deception Scenarios**

Overcoming Dependency on Detection

- **Eliminate dependency on detection** of an ongoing cyber-attack or on knowledge about an attacker

- **Deception Scenario is a product of local security policies**
  - Applicable deception scenarios are applied against actions beyond the scope of assigned authority (obtaining information about existing or non–existing resources)

- **Triggering deception scenarios based on Deception Rulesets**
  - Security Policy Violation (entering Deception Space)
  - Anomaly Detection (unusual behaviors – deviation from expected pre-defined behavior)
  - Enticement (“honey-paths”)

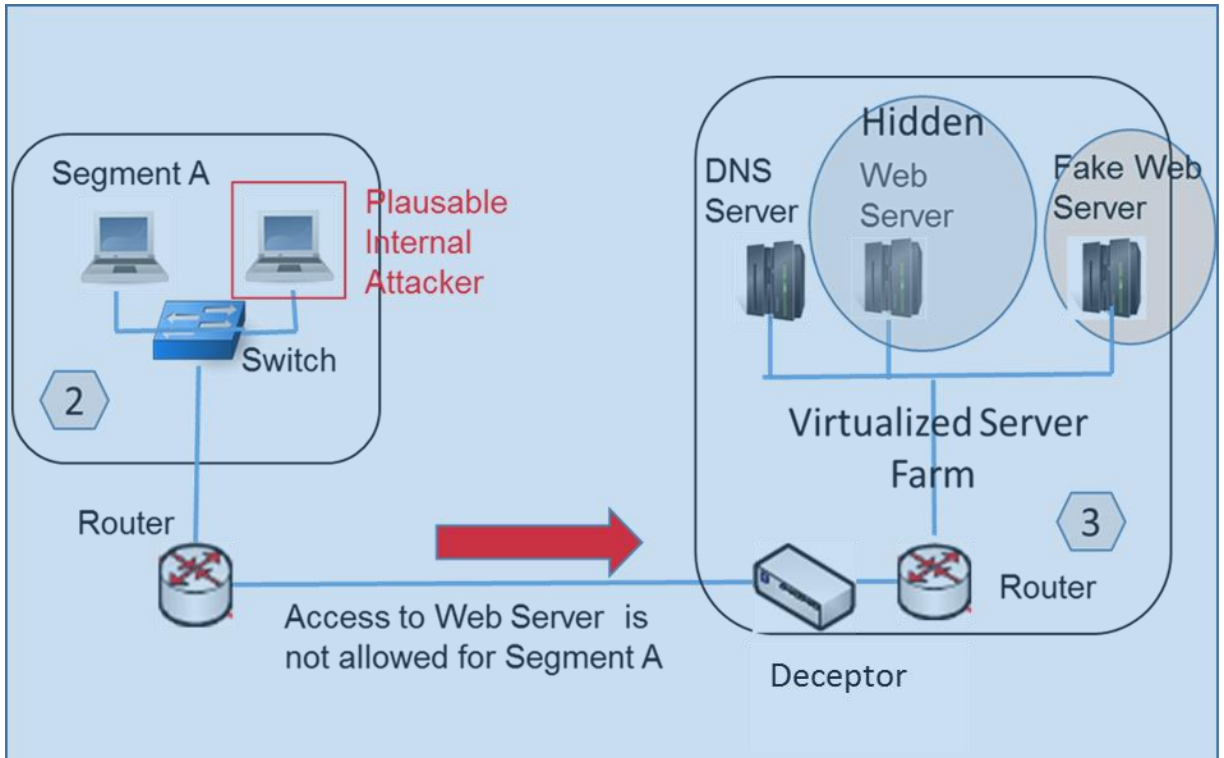
Deception Space and Security Policy

- **Security Policy**: defines boundaries of what are explicitly or implicitly disallowed
- **Deception Space**: domain of misinformation and network falsification derived from established security policy of a protected network
  - What to hide, what to falsify
  - Fictitious “security holes”
  - Configuration “errors”
  - Fictitious penetration paths (“honey-path”), fictitious access point
  - Do not affect the actual security posture of a target network.
- **Deception Auditing**: live monitoring of real and deception paths and points of access for feedback

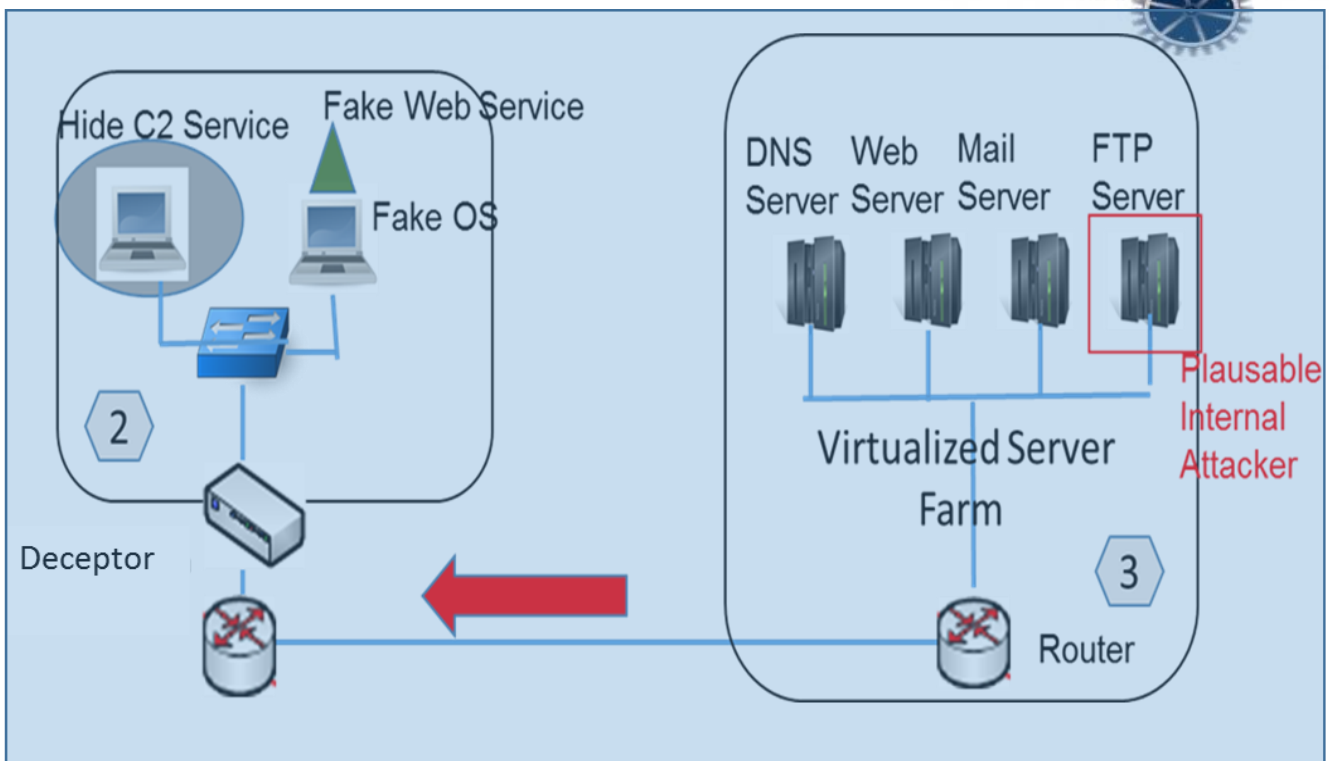
```
<ddl:Interface rdf:about="FAKE0:eth0">
<ddl:name>FAKE0:eth0</ddl:name>
<ddl:hasDeceptoType rdf:resource="MFake"/>
<ddl:hasProfile rdf:resource="FalseProfile1"/>
<ddl:locatedAt rdf:resource="FAKE0"/>
</ddl:Interface>

<ddl:Profile rdf:about="FalseProfile1">
<ddl:name>FalseProfile1</ddl:name>
<ddl:hasMacAddr rdf:resource="10.5.15.10/24"/>
<ddl:hasIPAddr rdf:resource="00:0C:29:45:67:89"/>
<ddl:hasGW rdf:resource="10.5.15.1/24"/>
<ddl:hasTTL rdf:resource="2"/>
<ddl:connectedTo rdf:resource="GW:eth2"/>
</ddl:Profile>
```

Triggering Deception: "Unauthorized" and "Unusual" Access



- No knowledge of a presence of an internal attacker
- The decoy "exists" only through the packet manipulations and responses manufactured by the Deceptor
- Stealth and minimal attack surface



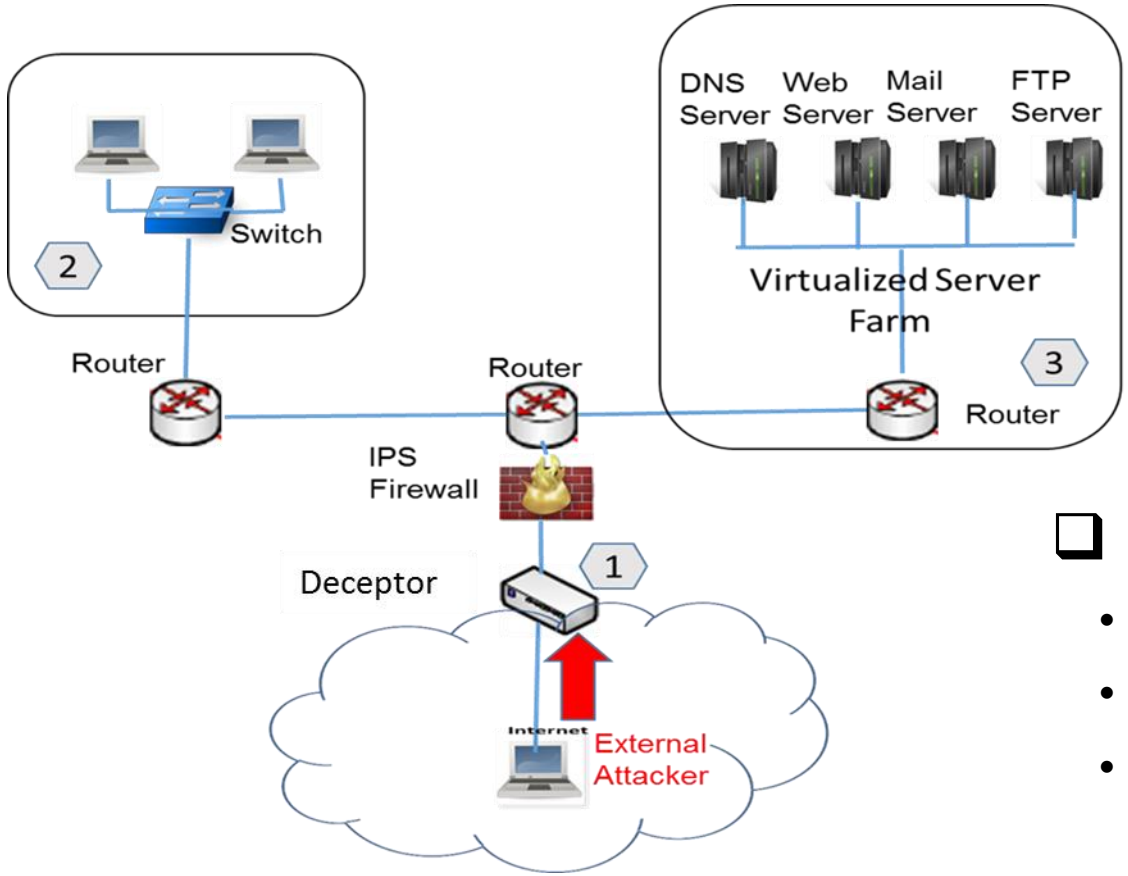
- No additional software is created or installed on those workstations
- The Deceptor manufactures all responses on behalf of those fictitious services

Deception Plot: Overcoming the Challenges

- **Dependency on cyber-attack detection and attacker's profiling**
  - Determines triggers of deception scenarios
  - There could be false positives
  - Attackers could be stealth
- **Coexistence / Interoperability with cyber defense controls**
- **Effectiveness of deployed deception**
  - Verifiability of deception story
  - Deception longevity and sustainability
  - Deception devices are subjects of attacks
- **From Localized Deception to Enterprise-wide Deception Scenarios**

Coexisting with a Firewall

❑ Is Deceptor a "Firewall on Steroids" ?



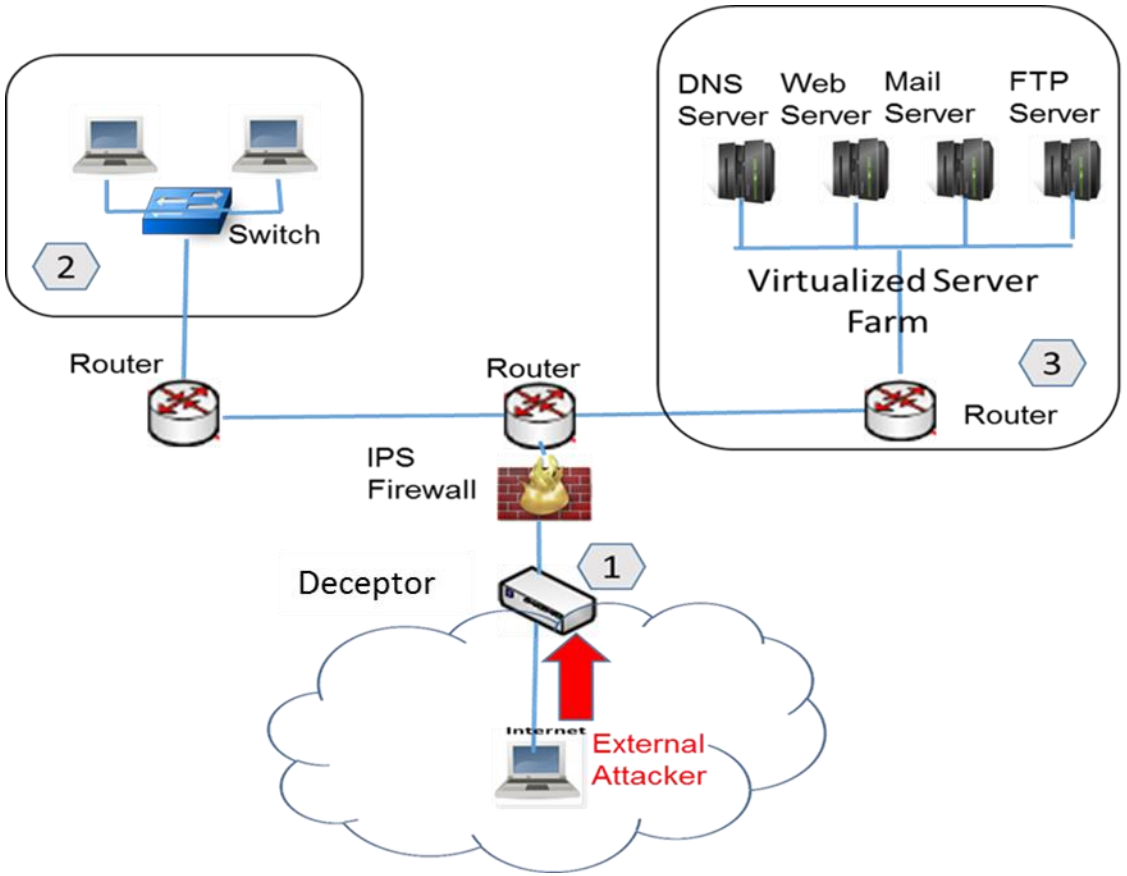
❑ Yes: Complimentary Plug-in Module

- Deception Space is a product of security policy
- Gartner report references deception as a part of firewalls

❑ No: Separate Deployment

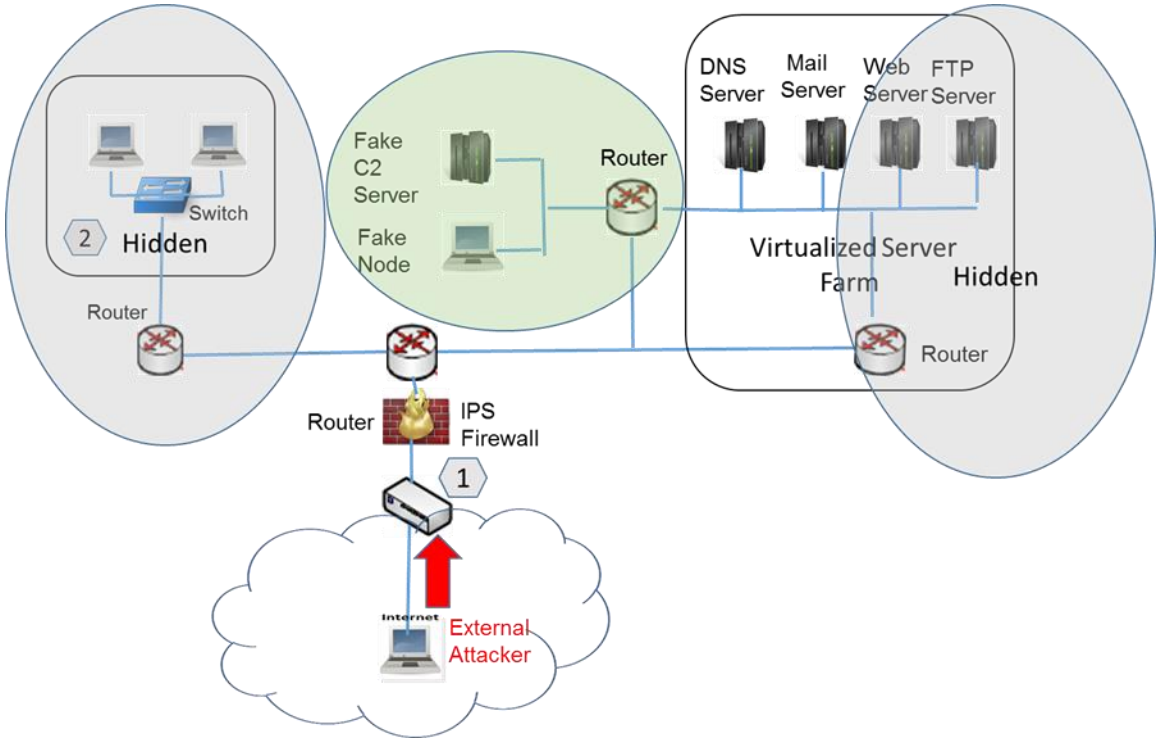
- Can be used in location where firewalls are not deployed
- Firewall also needs protection (firewalking deception)
- Deceives an external attacker about firewall's access-control rules and the type of firewall

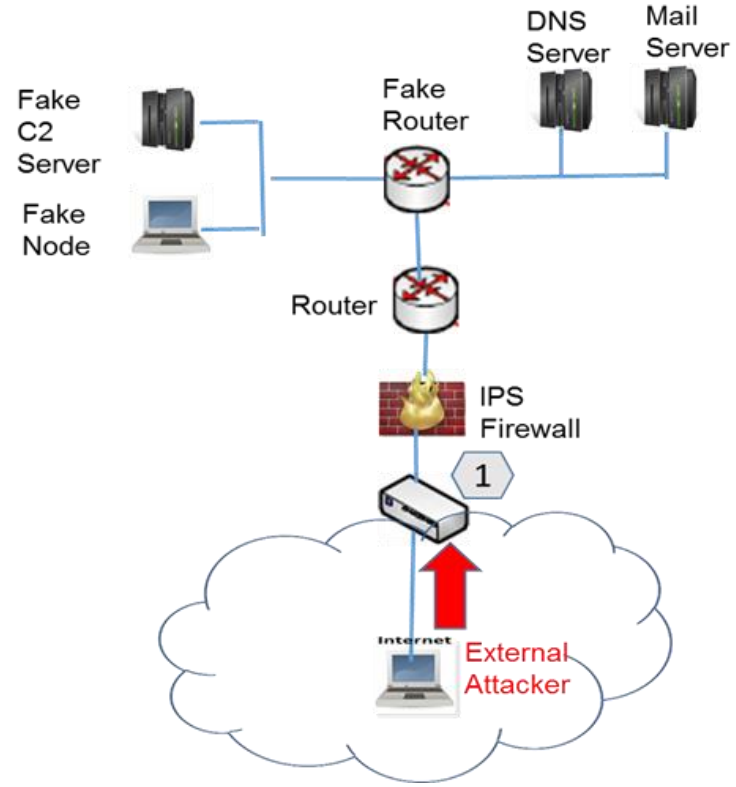
Deception Plot: Separate Deployment



- **Deception Channels**: traceroute, ACL detection, mapping probes, etc.
- **Deception Elements**: manufacturing network protocol responses on behalf of the firewall, hosts and devices behind the firewall
- **Example Deception Story**: misleading an attacker about firewall configuration/capabilities :
  - Allow certain TCP/UDP traffic through the firewall or disallow TCP/UFP traffic if it is intended for non-existing or non-exposed internal hosts;
  - Disable stateful inspection on the firewall;
  - Enable certain ICMP messaging through the firewall;
  - Expose fake routers, hosts and subnets/

Deception Plot: Separate Deployment





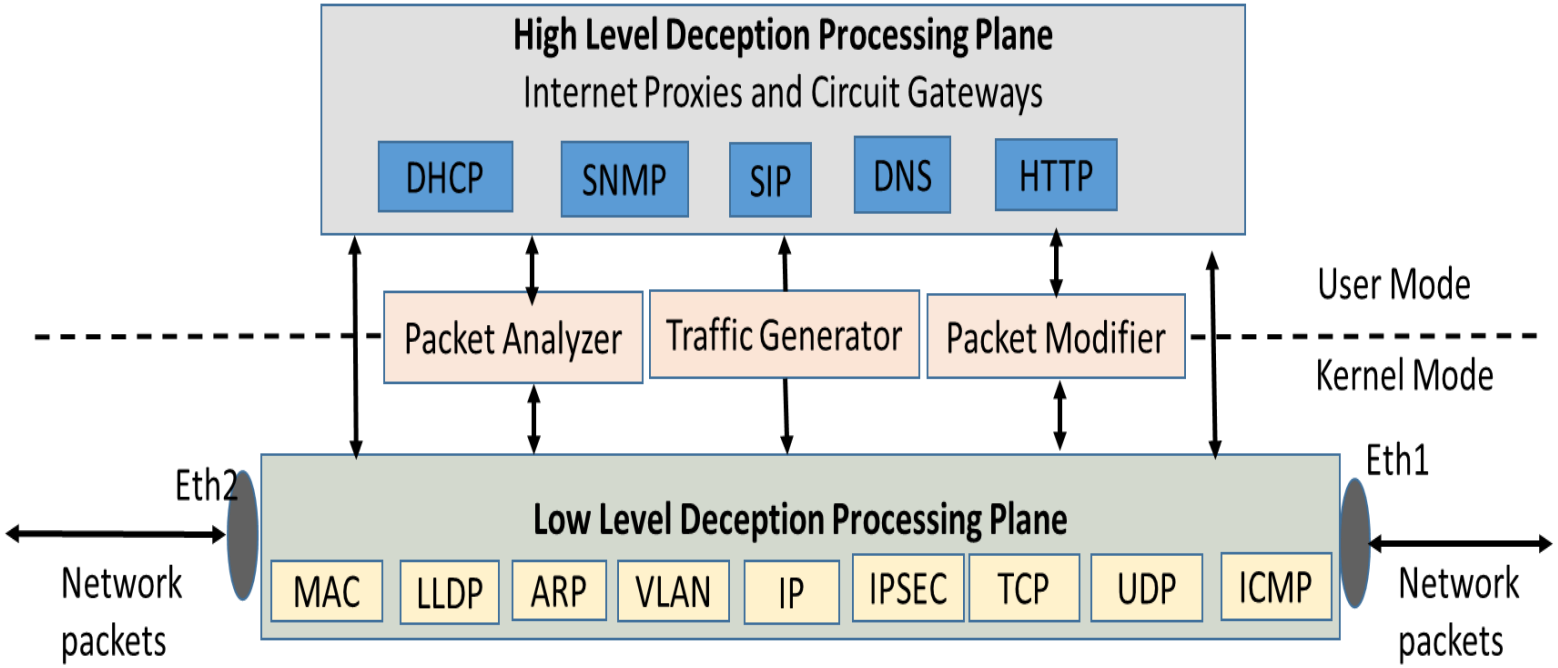
- Misleads the attacker about ACLs, rulesets and capabilities of a target firewall
- Resistant to co-opting by attackers, minimal dependencies, no trust relationship between a Deceptor and a firewall

Deception Plot: Overcoming the Challenges

- **Dependency on cyber-attack detection and attacker's profiling**
  - Determines triggers of deception scenarios
  - There could be false positives
  - Attackers could be stealth
- **Coexistence / Interoperability with cyber defense controls**
- **Effectiveness of deployed deception**
  - Verifiability of deception story
  - Deception longevity and sustainability
  - Deception devices are subjects of attacks
- **From Localized Deception to Enterprise-wide Deception Scenarios**

Verifiability of Deception Story

- Consistency of discovery across multiple network channels through which a deception story is revealed and verified by an attacker.
- Diverse set of techniques used simultaneously for cross-references and confirmation
- Identification of attacker's observation channels and sources to convey the deception to the adversary.



- ✓ Monitors and generates the ingress and egress network traffic though
- ✓ OSI Layer 2 -7 packet inspection
- ✓ Manipulate intercepted network packets and selectively craft responses on behalf of real and fake nodes /services
- ✓ Feedback through monitoring deception paths

Deception Longevity and Sustainability

- **Protocol Equivocation:** adding more uncertainty
- **Considering cognitive bias in projected deception effects**
- **Dynamic Cyber Deception:** perception of dynamic (transient) environment
- **Multi-layered and multi-phase deception scenarios**
  - Throughout entire network segment
  - Across cyber kill chain phases

Protocol Equivocation

- Creates uncertainty and inconsistency in network and system responses by dynamically inserting and removing failures and successes in message exchanges
  - Simulated network protocol message exchange failures (“tools failures”);
  - Intermittent errors and response delays
- Monitors and manipulates OSI Layer 3-7 protocol packets
  - Selectively blocking or passing message traffic
  - TCP and UDP Protocol fields alterations
  - Dynamically changing IP headers fields (checksum, TTLs, etc.)
  - Generating superfluous and false protocol messages
  - Introducing artificial timing delays

Protocol Equivocation Benefits

- Not aimed at defeating a particular set of techniques
- Especially effective against automated attacks(especially during internal reconnaissance)
- Not vulnerable to a “deception explosion”
- Creates ambiguity and uncertainty in attacker’s perception of a target network
- Delays an attacker at each step of reconnaissance and enforces inconsistency across different probes
- Can be used in in conjunction with other techniques when deception activity is already in progress

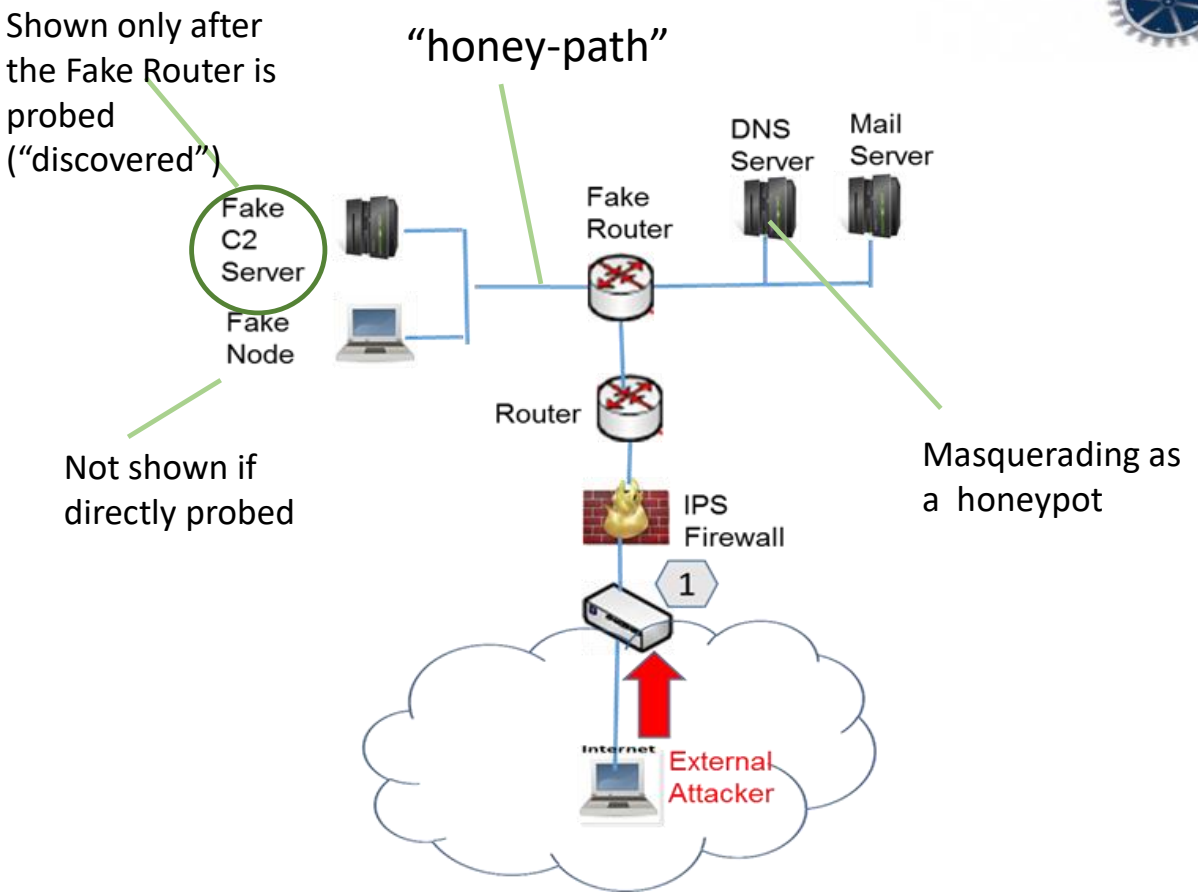
Cognitive Bias, Deception Construction and Effects

❑ Conjunction Fallacy Bias

- Constructing deception elements exposed to an attacker as pieces of a puzzle (“hiding the fiction”)

❑ Confirmation Bias

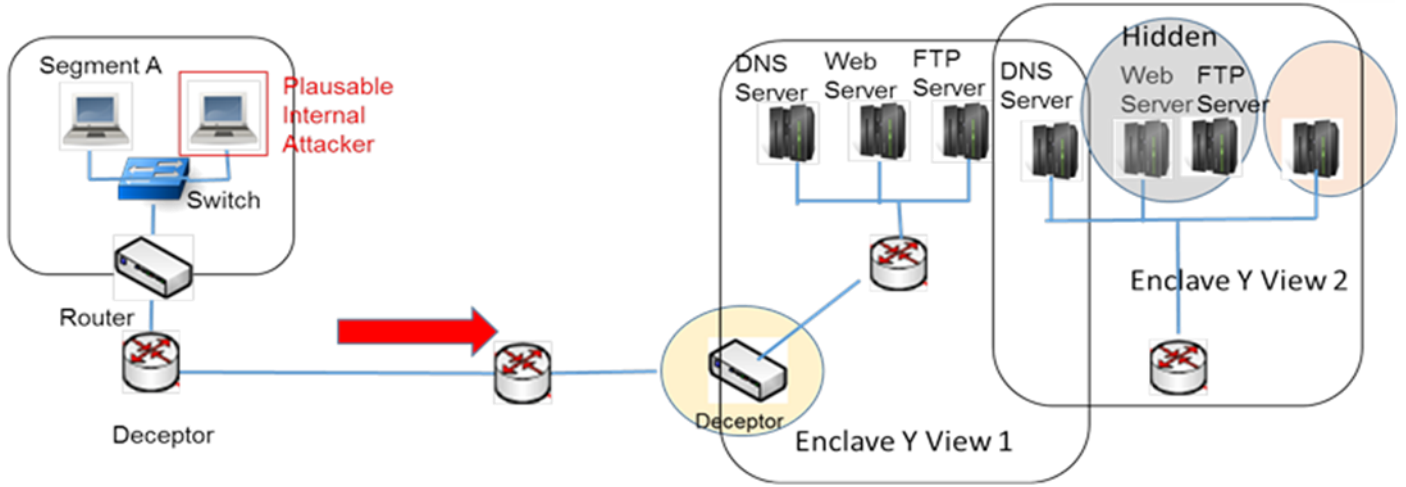
- Manipulating over-confidence: from “revealing the fiction and concealing the truth”, to **“hiding and exposing the fiction”**
- Manipulating under-confidence: explicit deception raises doubts about validity of data already obtained by the adversary
- Protocol Equivocation: simulating (expected) network and protocol failures
- “Masquerading the real”: hiding the real by showing it to be a false.



Presenting and monitoring configurable fictitious penetration paths (“honey-path”) and fictitious points of access to a potential attacker

Dynamic Cyber Deception

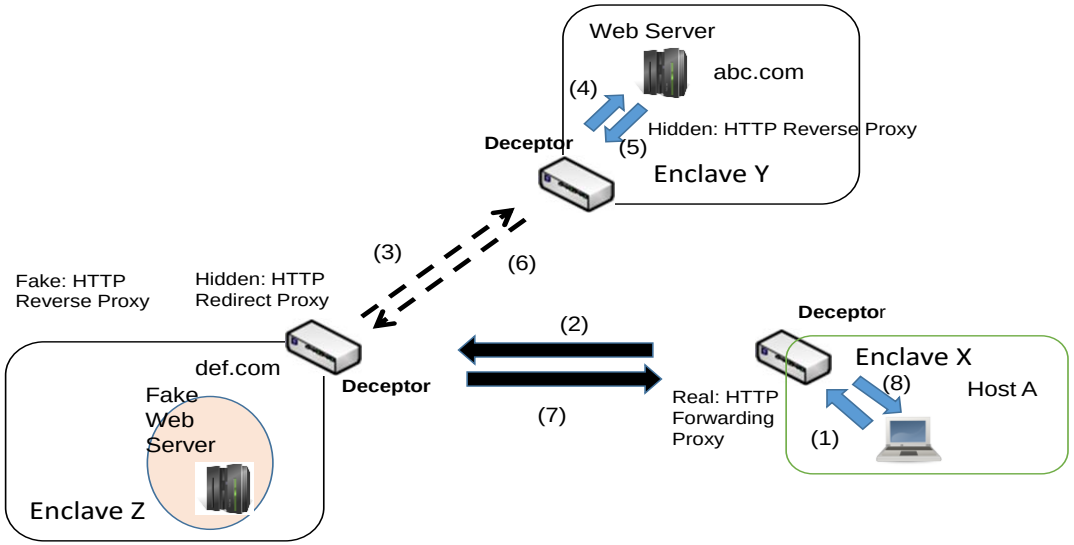
- Create a perception of a transient network environment for inconclusive reconnaissance results



- Dynamic Deception Views
  - Multiple deception configurations.
  - Inconclusive network attack surface across consecutive probes)

- Web Traffic Deception and Misdirection
  - Mutating transparent proxies (caching, reverse, redirectors/forwarders) to pollute service traffic patterns

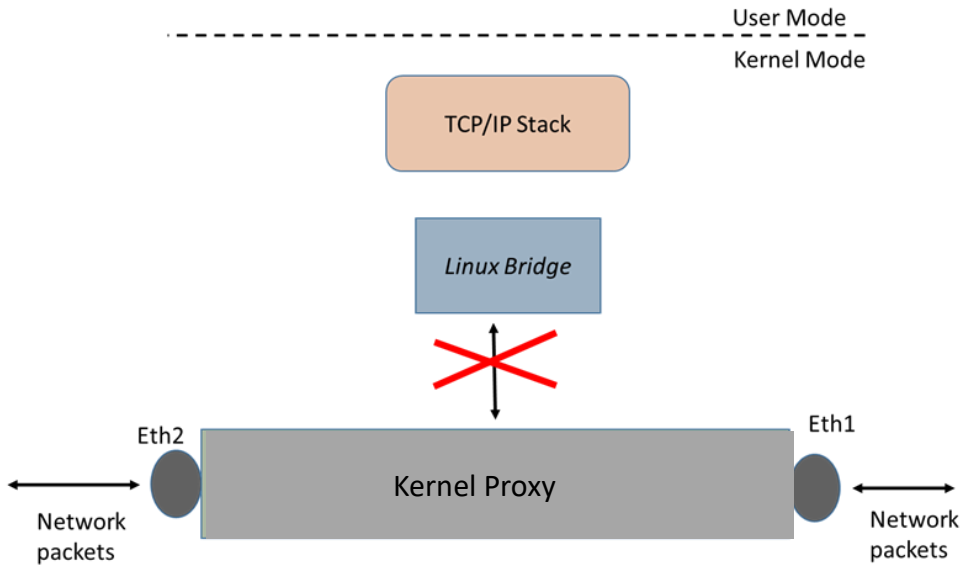
- DNS Information Hiding



Platforms for Deception Stealth

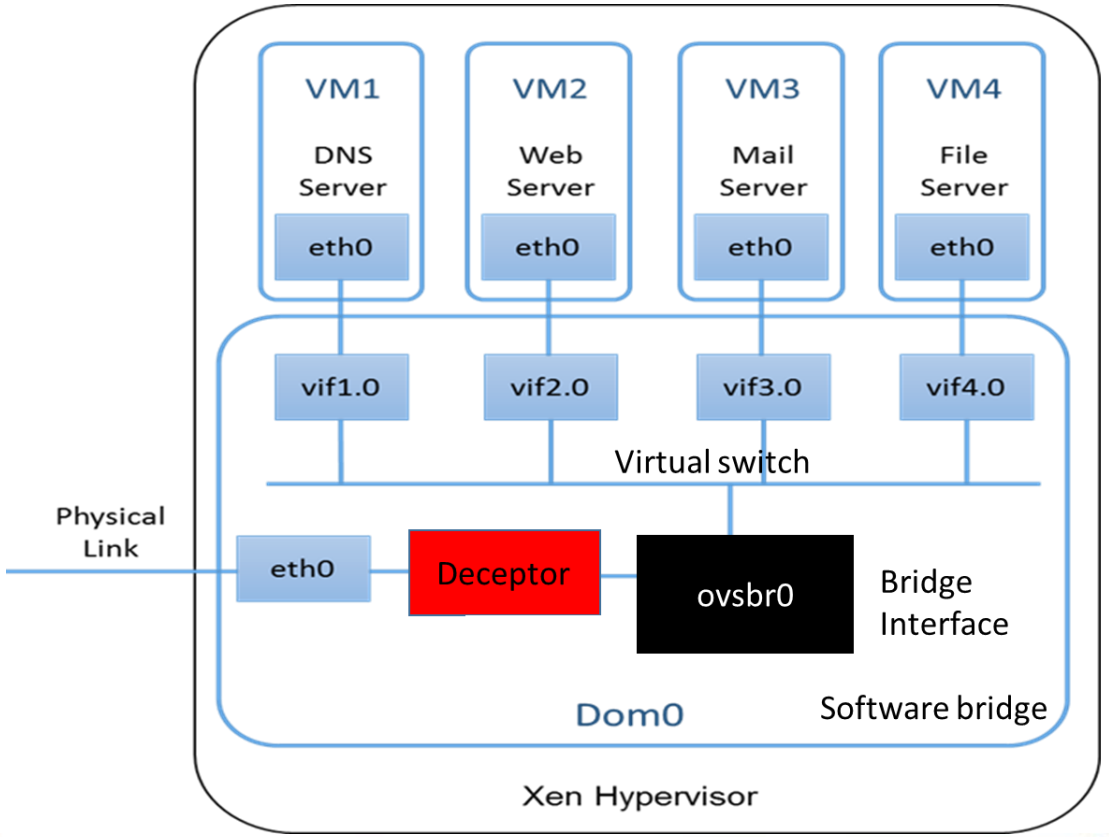
❑ Stand-alone transparent network appliance

- Transparent network **bridge**: stealthy, **small attack surface**
- Placed at the edge of a network segment
- In-line mode, bump-in-the-wire



❑ Xen Virtualized Environment

- Plug-in software module
- Deceptor intercepts all ingress and egress network packets to/from virtualized server/farm **bridge**

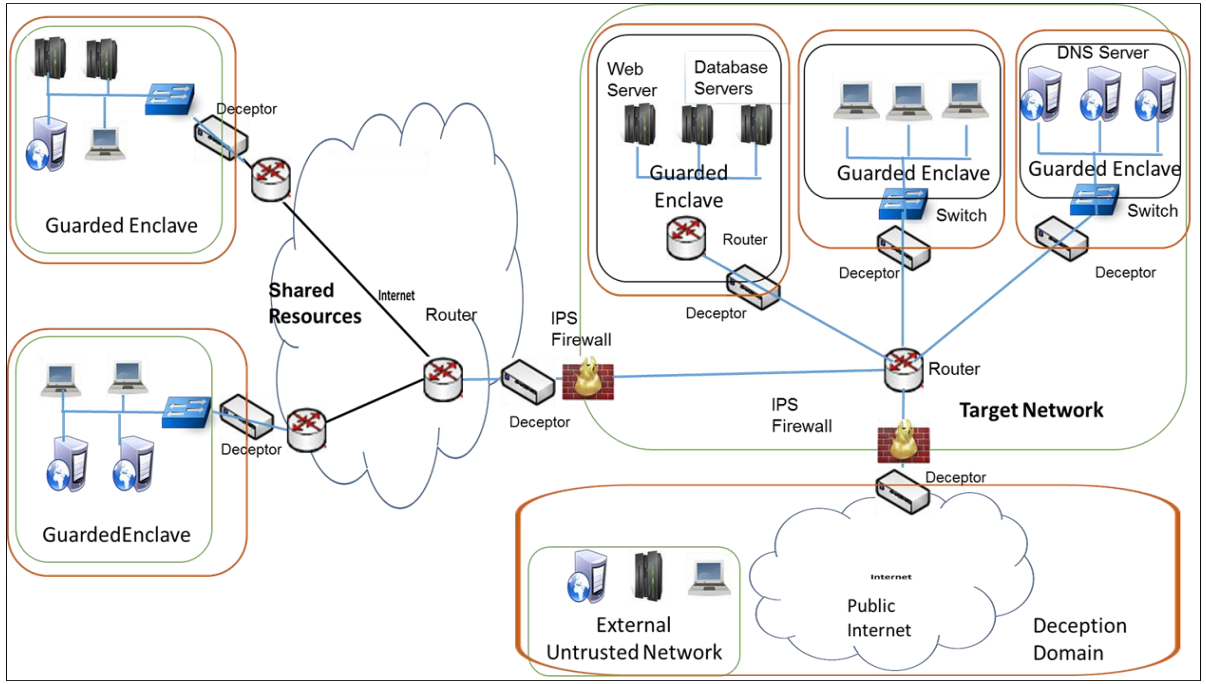


Deception Plot: Overcoming the Challenges

- **Dependency on cyber-attack detection and attacker's profiling**
  - Determines triggers of deception scenarios
  - There could be false positives
  - Attackers could be stealth
- **Coexistence / Interoperability with cyber defense controls**
- **Effectiveness of deployed deception**
  - Verifiability of deception story
  - Deception explosion
  - Deception devices are subjects of attacks
- **From Localized Deception to Enterprise-wide Deception Scenarios**

From Local to Enterprise-scale Deception

- **Deception Domain Model :** creating fragmented, obscured and evidentiary contradictive network viewpoints relative to attacker's location



Deception Policy:
- Defines how a given Guarded Enclave is presented to other Enclaves;
- Generated for each Deceptor
- Each Enclave is presented a different view of the same Guarded Enclave

Enclave:
- Deception domain comprised of one or more physical network segments;
- Logical network domain, in which provenance of each packet initiated from any node inside the enclave's boundary can be confirmed as originated from this enclave
- Each enclave is screened by Deceptor
- Part of the anti-spoofing verification chains

Guarded Enclave:
- Shielded by a Deceptor;
- Subject of a deception story

Deception Domain:
- Bound by a Deceptor(s);
- Subject to deception

- **Spoofing Mitigation**: creating and verifying network provenance

Lessons Learned

❑ Deception against a particular set of techniques does not scale well

- Exponentially increasing complexity of deception algorithms, overlapping techniques
- Spoofing diversity, timing variants

❑ More Practical Approach: Constructing Deception Story

- Deception Space and Security Policy, Deception Domain Model: Deception Views, Enclave Authentication
- Flexible Rulesets for presentation of deception information to an attacker, based on:
  - ➢ Initial deception objectives according to the local security policy and mission requirements,
  - ➢ A feedback received and reported by deception and 3rd party monitoring systems during deception deployment

❑ Multi-Layered and Multi-Phase Deception Scenarios

- Multiple deception units with coordination and synchronization of deception activity across the enterprise
- Deception explosion mitigation (Protocol Equivocation, Exploiting Cognitive Bias, MTD Deception)
- Greater protocol support for deception verifiability

Future Work

- Bridge the gap between high level reasoning of deception scenario and deception elements applicable to the low-level implementations.

- Scripting meta-language for formal descriptions of desired deception scenarios
  - **Deception Space** based on network and software attack surface analysis, security policy and network configuration,
  - **Desired Responses** of the system based on possible attacker scenarios, existing network infrastructure and the specific user requirements.
  - **Deception Back Channels** (direct or indirect) to relay deception back to the attacker.
  - Mapping ontological constructs for deception taxonomy into deception techniques and methods

- Parser and Translator to create configuration data and assemble modular deception executable modules

Questions and Discussion