efficient iP™
DEFINING SMART DDI

Webinar

Five Key Ways to Increase Network Security

Agenda

- **Introduction: DNS and BYOD Security Challenges**
- **Five Tactics to Secure the Network Infrastructure**
  - Tactic 1: Apply Best Practices
  - Tactic 2: Enable DNSSEC
  - Tactic 3: Mitigate the Security Risks of BYOD
  - Tactic 4: Protect Against Malware with DNS Firewall
  - Tactic 5: Deploy a Consistent IP Topology
- **About EfficientIP**

New Security Risks Demand New Solutions

- Cyber Attacks Are in Constant Growth: +42% Last Year*
- Most of the Attacks Rely on the Domain Name System (DNS)**
- DNS Based Malware Circumvents Traditional Security Defense
- BYOD Is Increasing the Threat

*Symantec: Internet security threat report 2013
** Internet Software Consortium, Paul Vixie

What Is at Stake?

Business Continuity

Intellectual Property Theft

Damaged Reputation

Password Stealing

Legal Issues

Tactic 1:
Apply Best Practices

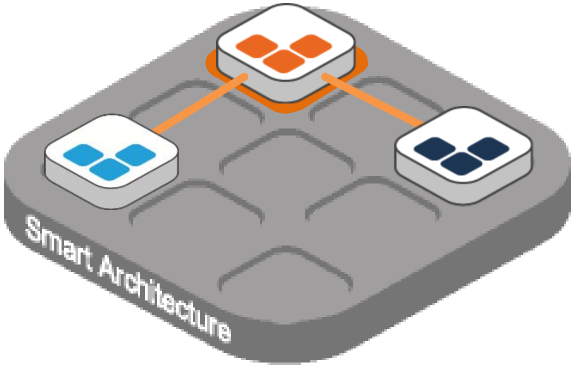
Enforce Best Practices configurations

- Run Up-to-date DNS Software Version
- Separate the Functions Caching, Resolver and Authoritative as Possible
- Use Data Flow Identification and ACLs to Control How and What Information is Published

Deploy a Stealth DNS Architecture

Principle

- A DNS slave server is published to DNS clients as the Master DNS server
- DNS Master server is hidden to DNS clients behind firewalls



Hidden DNS master

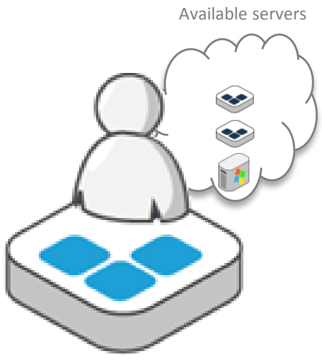
DNS Pseudo Master (Slave)

DNS Slave server

Benefits

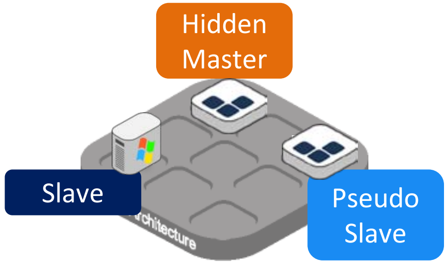
- The Master server remains protected from attacks
- DNS Data and then service cannot be corrupted

Apply State-of-the-Art Design & Enforce Best Practices



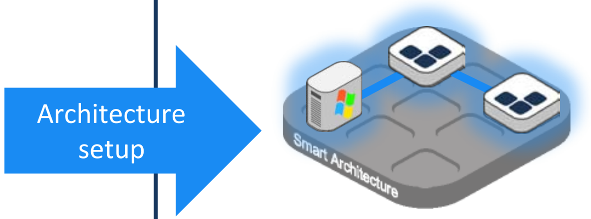
Management Appliance

1.Design



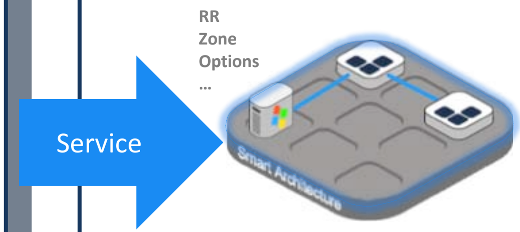
Stealth DNS Template

2.Deploy



Stealth DNS Template

3.Manage

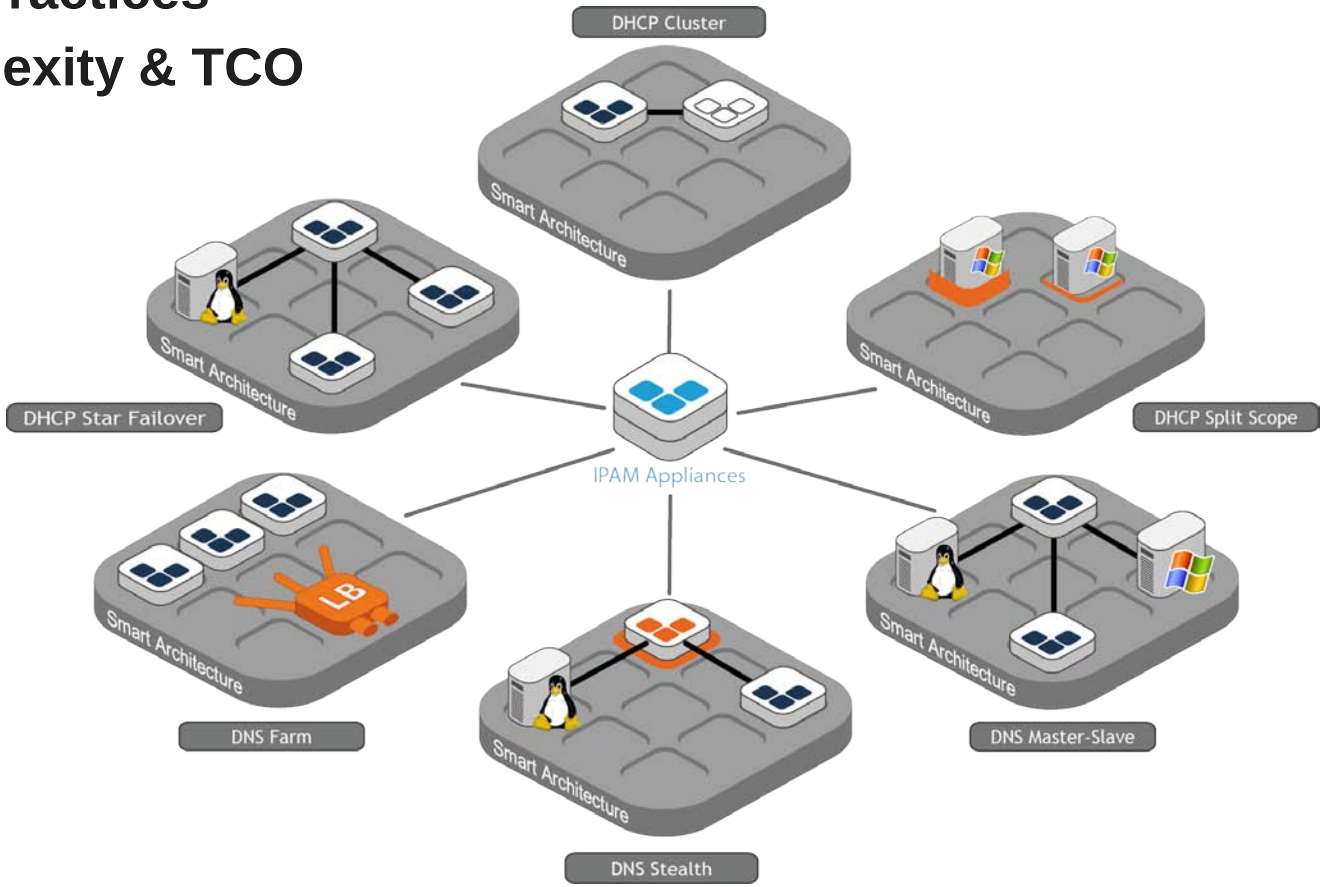


Stealth DNS Template

Management of the SmartArchitecture as one “Virtual server”

SmartArchitecture™
Secure, Reliable, Automated

- Automate Deployment and Management
- Enforce Best Practices
- Reduce Complexity & TCO



Tactic 2:
Enable DNSSEC

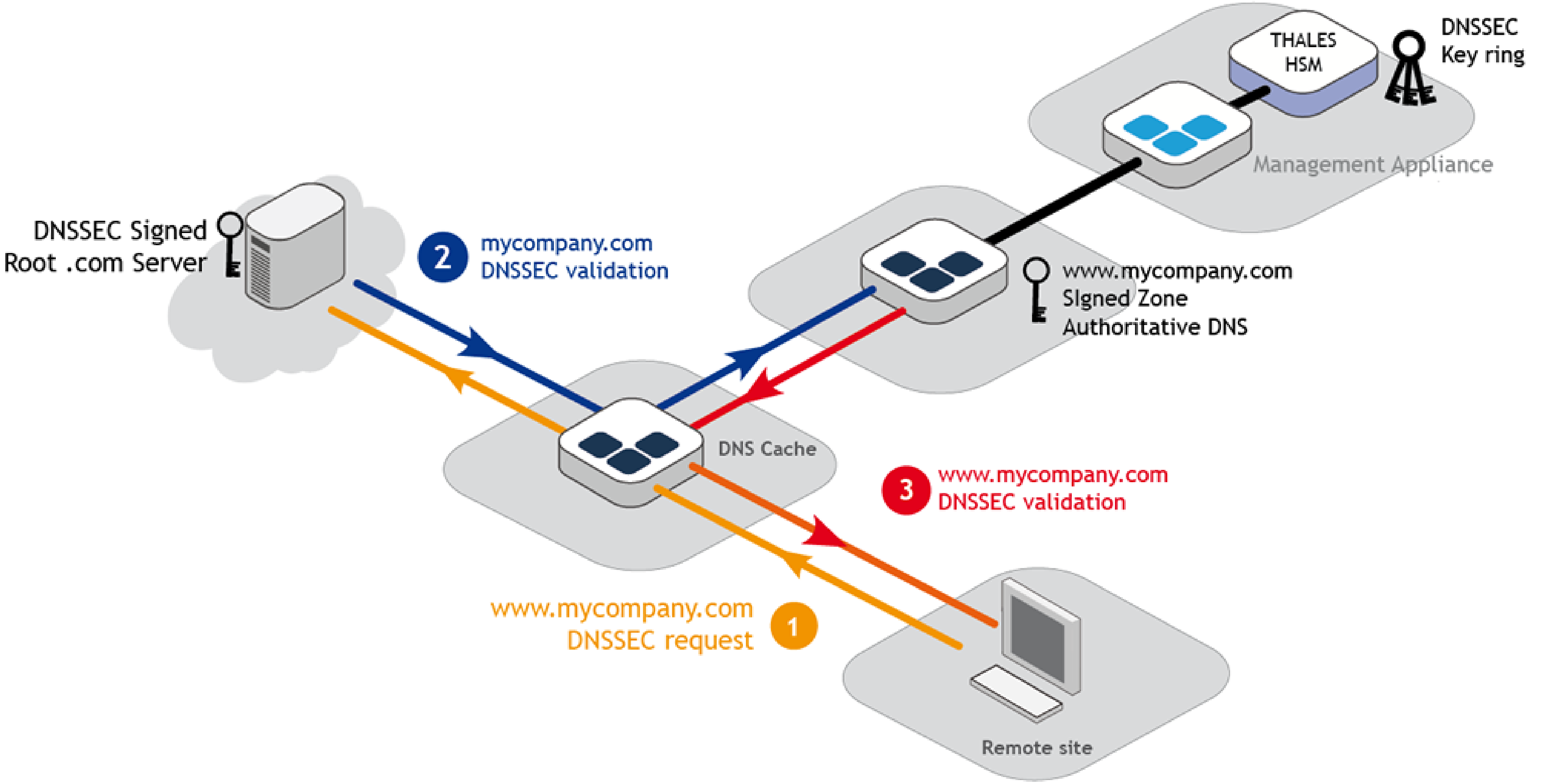
What is DNSSEC?

- DNSSEC is an extension of the Domain Name System (DNS), designed to ensure authenticity and integrity of DNS data answers.
- DNSSEC authenticates data source and data content
- DNSSEC is based on the exchange of keys inside specific signed resource records
- DNSSEC is recommended by Internet top level authorities (ICANN)

DNSSEC Challenges

- Setting up DNSSEC correctly is **complex.**
- If incorrectly set up, it may cause **unavailability of services** (dark zone)
- A rollback is very **hard**.
- Compromised key may lead you to **trust attackers.**
- ➔ it is therefore mandatory to **ensure best practices are respected.**

EfficientIP DNSSEC Solution



EfficientIP DNSSEC Solution

- Automates DNSSEC administration
- Simplifies signature of zones
- Applies DNSSEC Best Practices
- Uses latest cryptographic standards
- Normalizes keys management procedure
- Enhances reliability of delegation (TLD)

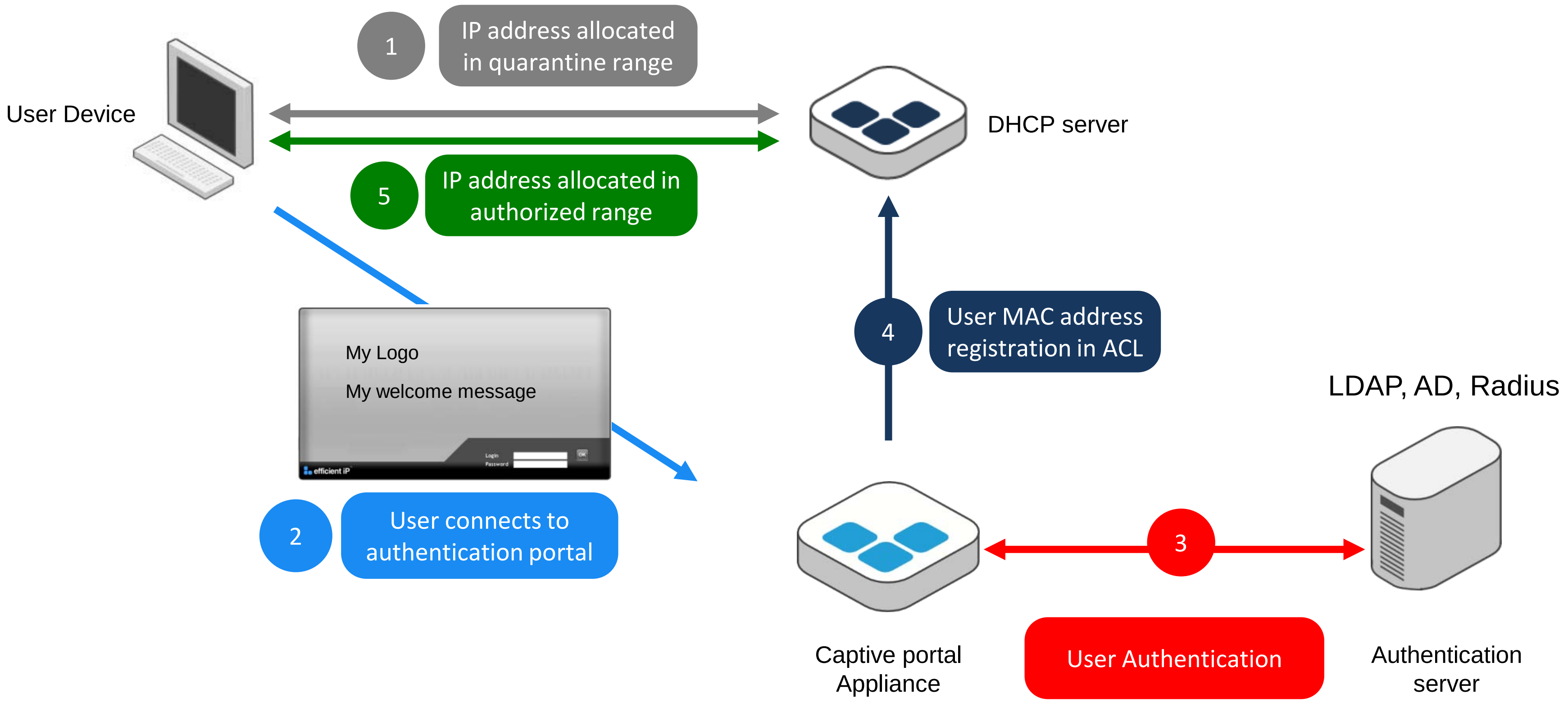
Tactic 3:
Mitigate the Security Risks of BYOD

BYOD Vulnerabilities

- **External Devices are Given Access to the Company's Internal Network**
  - Limited device protection outside of the corporate network
  - No control over what is downloaded on the devices
  - No control on device security updates

Captive Web Portal

Control User Access to Network Services



User Device

DHCP server

1 IP address allocated in quarantine range

5 IP address allocated in authorized range

2 User connects to authentication portal

4 User MAC address registration in ACL

3 User Authentication

LDAP, AD, Radius

Captive portal Appliance

Authentication server

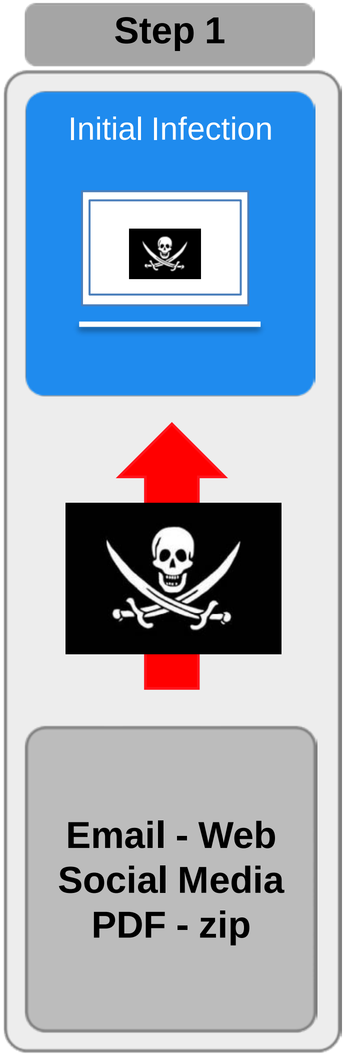
My Logo

My welcome message

Tactic 4:

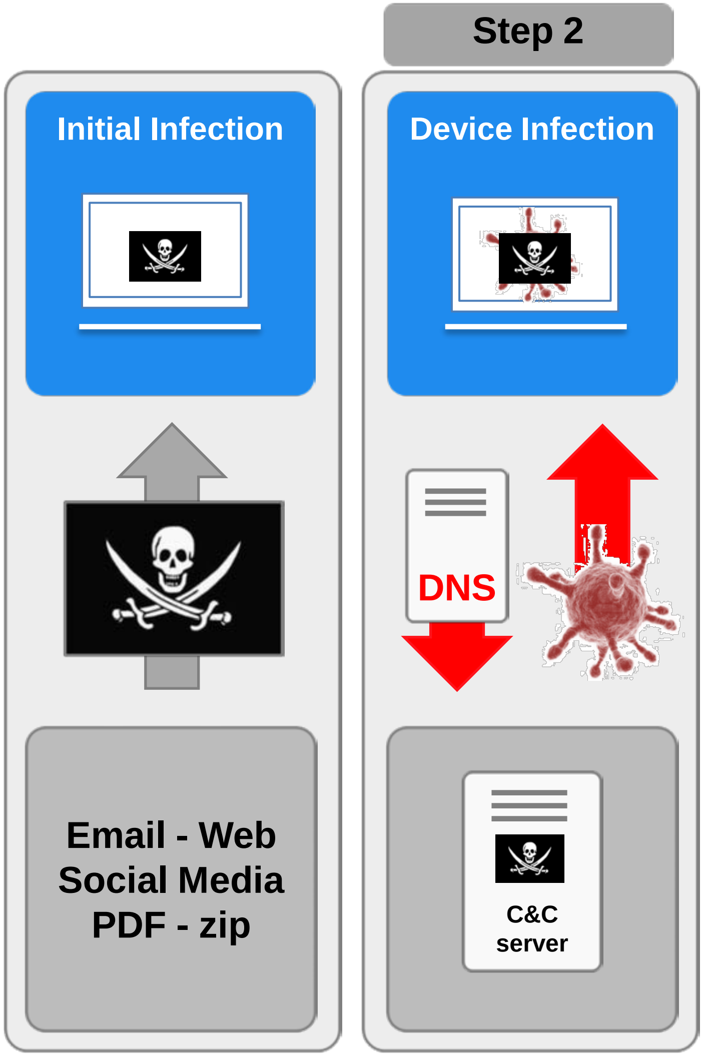
Protect Against Malware with DNS Firewall

How Do Malware DNS-Based Attacks Work?



Initial infection installed a part of the malware program

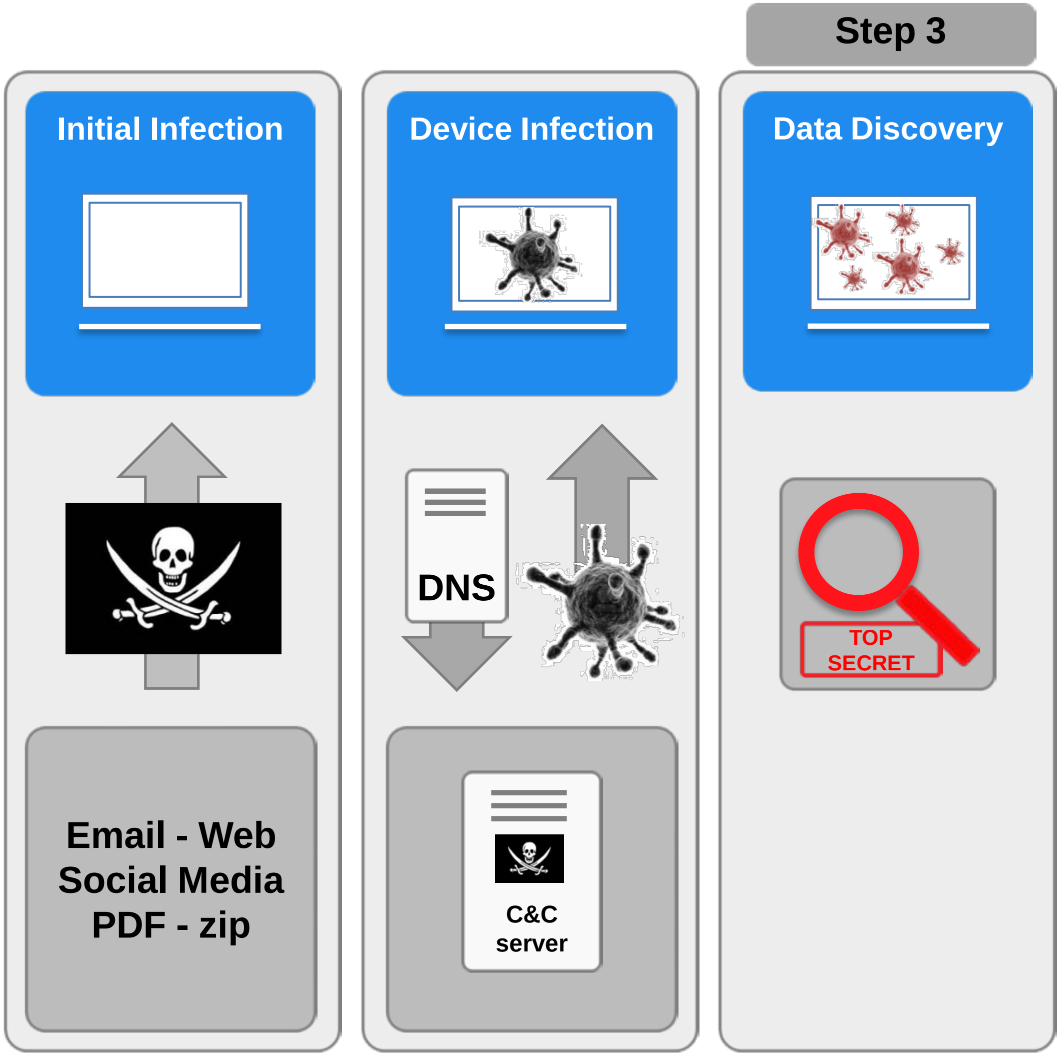
How Do Malware DNS-Based Attacks Work?



Download full malicious program

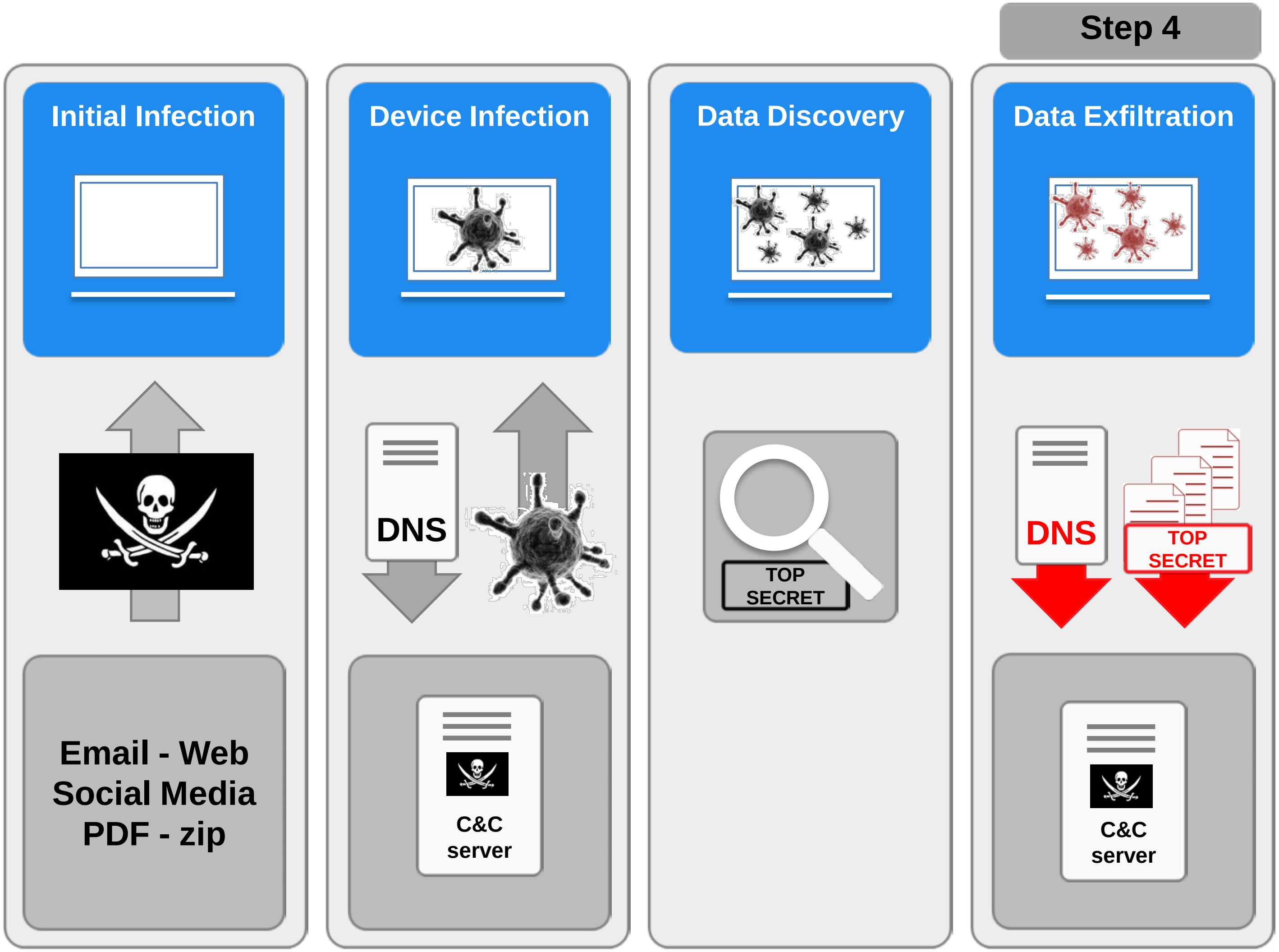
Malware program uses DNS service to Connect Hacker Server

How Do Malware DNS-Based Attacks Work?



DNS Based Malware Scans Enterprise Infrastructure

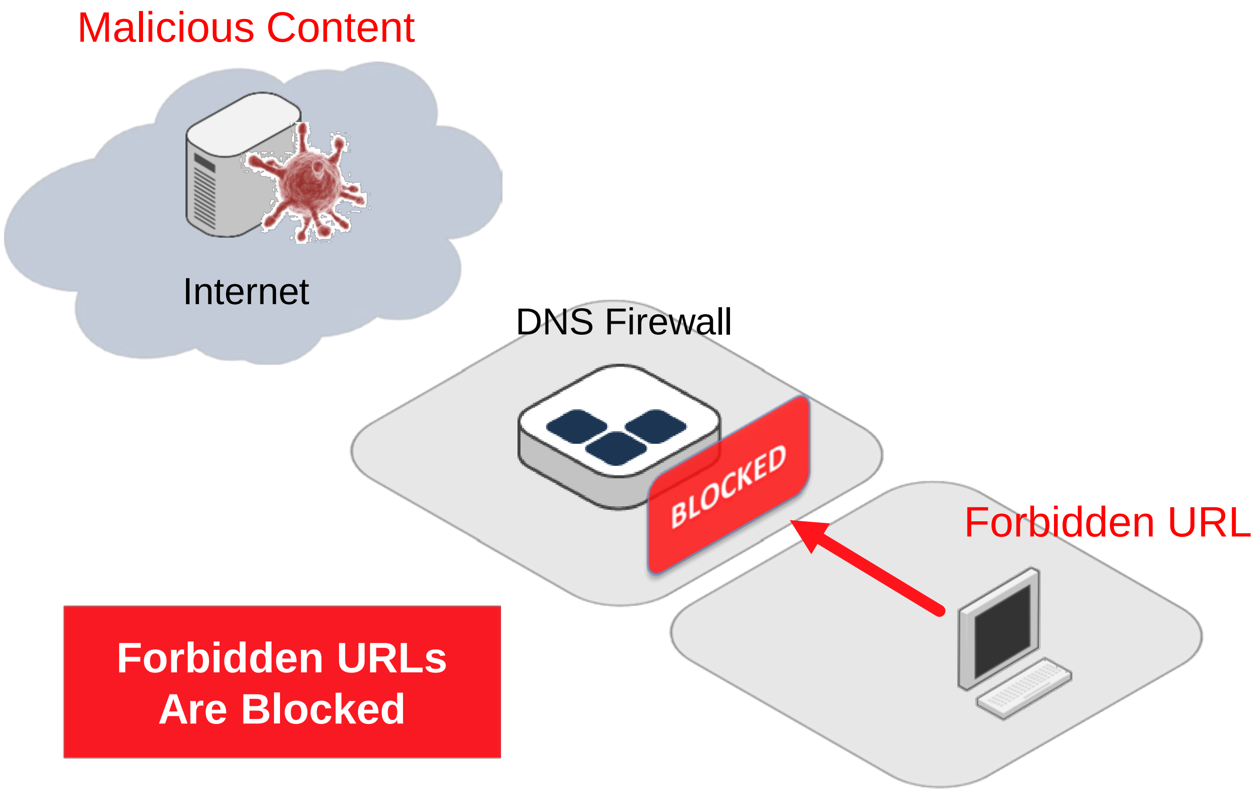
How Do Malware DNS-Based Attacks Work?



Data Exfiltration Using DNS Services

EfficientIP DNS Firewall

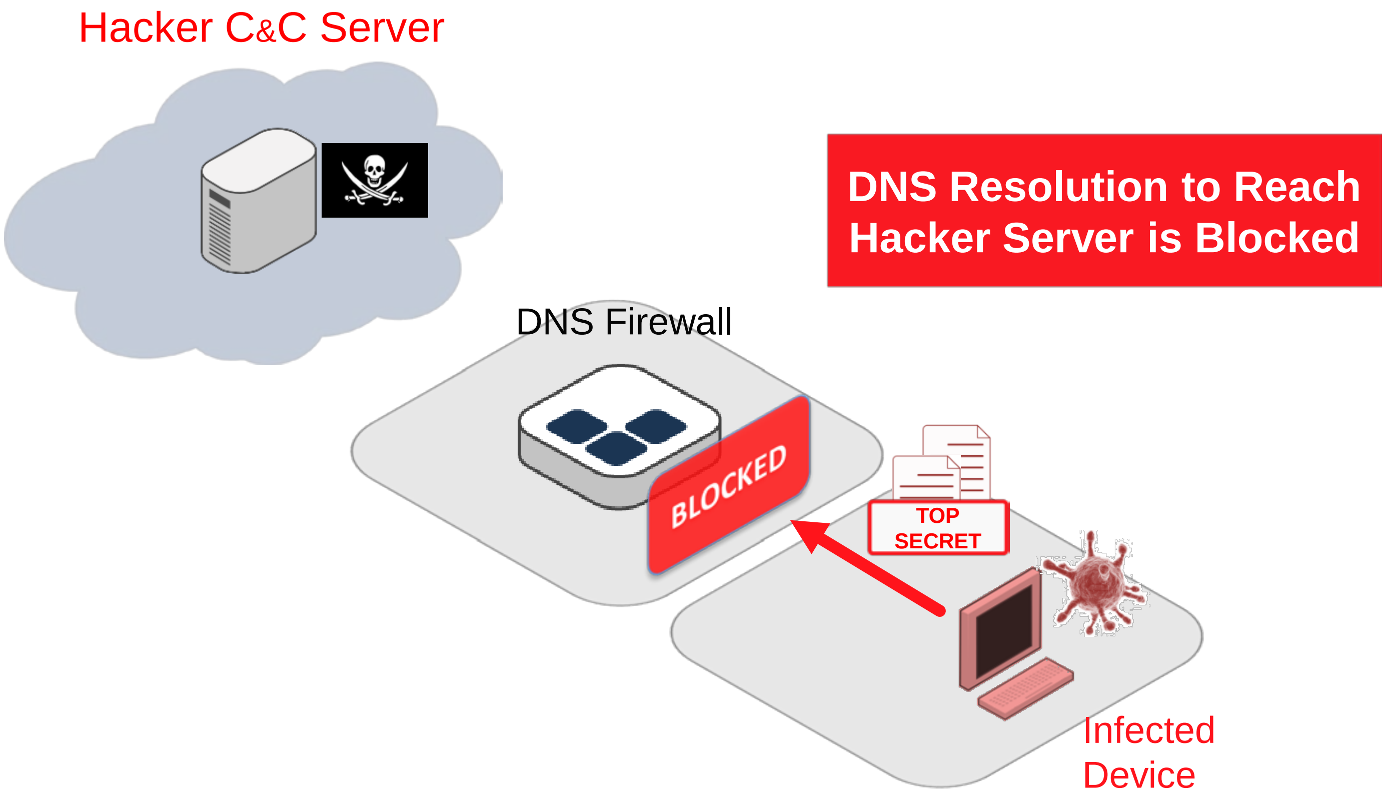
Prevent Initial Infection



Forbidden URLs Are Blocked

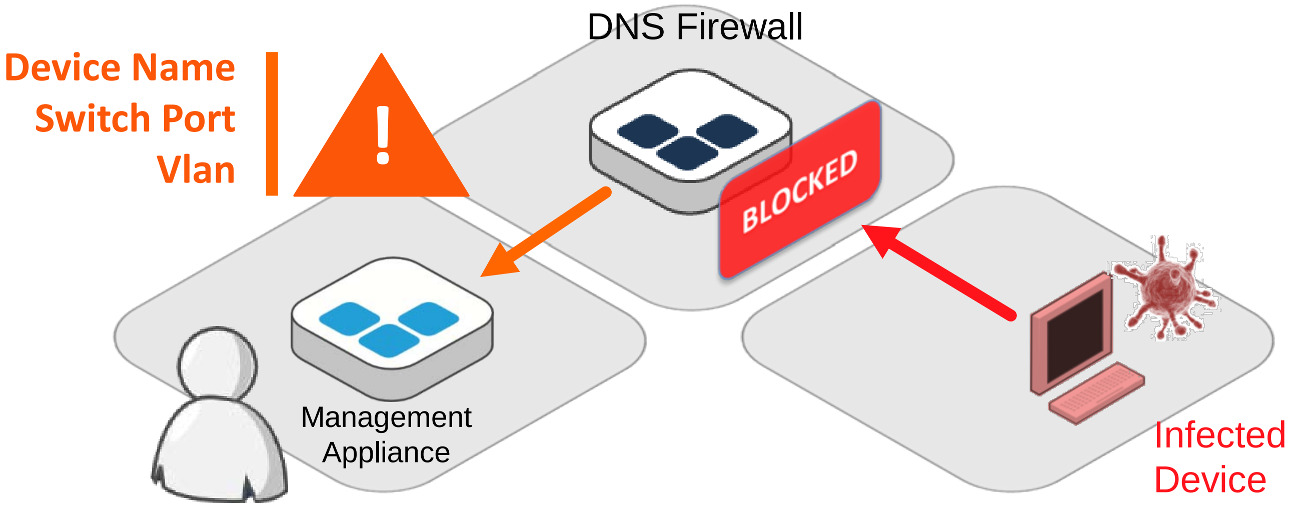
EfficientIP DNS Firewall

Mitigate Infected Devices And Data Exfiltration



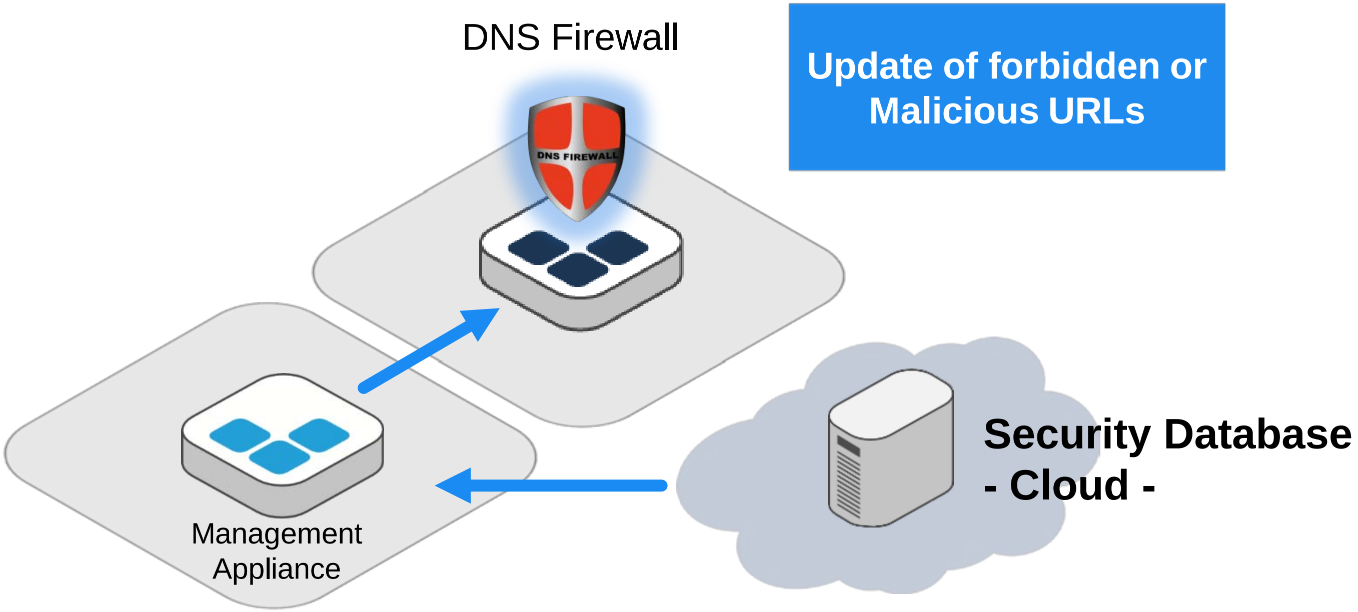
EfficientIP DNS Firewall

Locate Infected Devices And Alerts



EfficientIP DNS Firewall

Automated Up-to-Date Protection



EfficientIP DNS Firewall Benefits

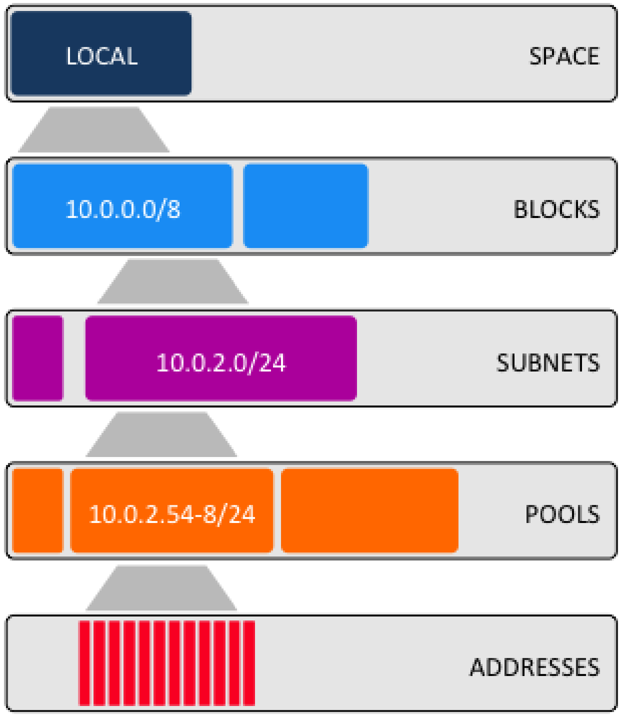
- Proactively Prevent New Attacks
- Detect and Block Malware Activity
- Identify and Locate Infected Devices
- Contain Malware Spreading

SOLID™ server

Tactic 5:
Deploy a Consistent IP Topology

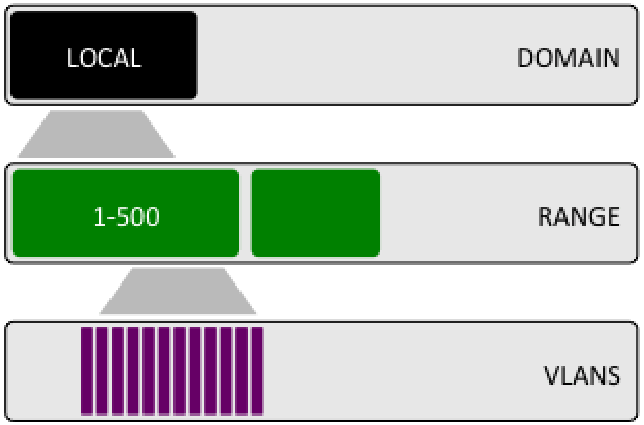
IPAM Design

- **IP Space**
  - Logical container of IPv4-v6 resources
  - Hierarchical resource organization
- **Global Consistency and Uniqueness Control within an IP Space**
  - No duplicate IP address or subnet overlap
- **Flexible IP Addressing Plan Organization**
  - Tag resources to organize them logically
    - VDC, location, services...
  - Unrestricted modeling criteria
    - Geographical, technical, clients or mix,



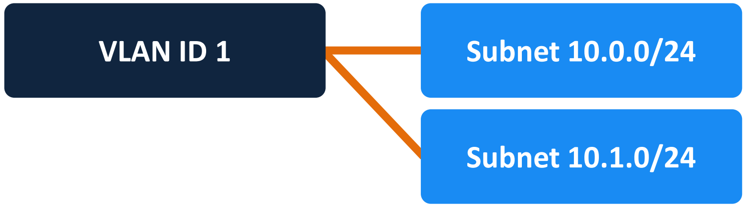
VLAN Design & Management

- **VLAN Domain Repository**
  - Logical container of VLANs
  - Hierarchical or flat organization
- **Flexible VLAN Organization Design**
  - Unrestricted modeling criteria
    - Geographical, technical, clients or mix,
  - Tag VLAN to organize them logically
    - VoIP, DC, location, services...



Unified IP Plan & VLAN Management

- **Assign VLANs to Subnets**
  - Find free/available VLANs



VLAN ID 1

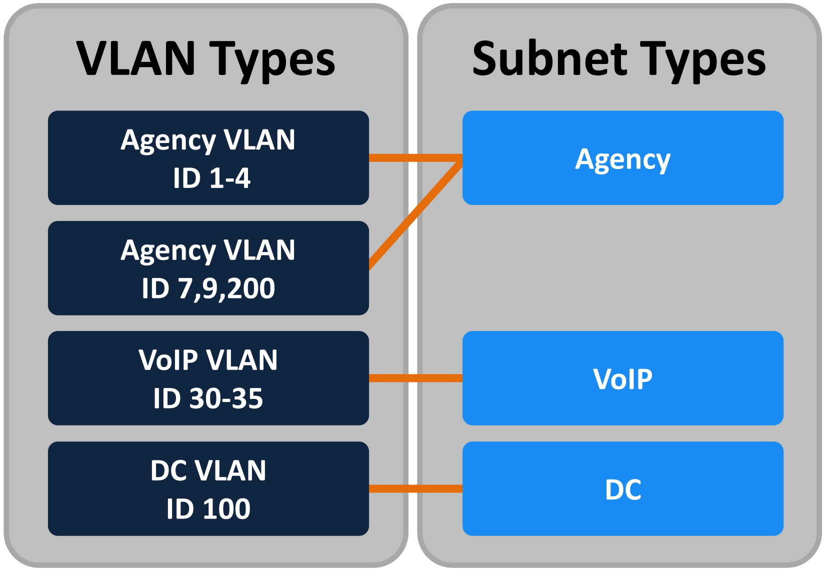
Subnet 10.0.0/24

Subnet 10.1.0/24

- **Define Assignment Policies**
  - Authorized VLANs to specific subnet type (Class)

IP and VLAN Plans Consistency Control

Automated & Unified Management



VLAN Types

Agency VLAN ID 1-4

Agency VLAN ID 7,9,200

VoIP VLAN ID 30-35

DC VLAN ID 100

Subnet Types

Agency

VoIP

DC

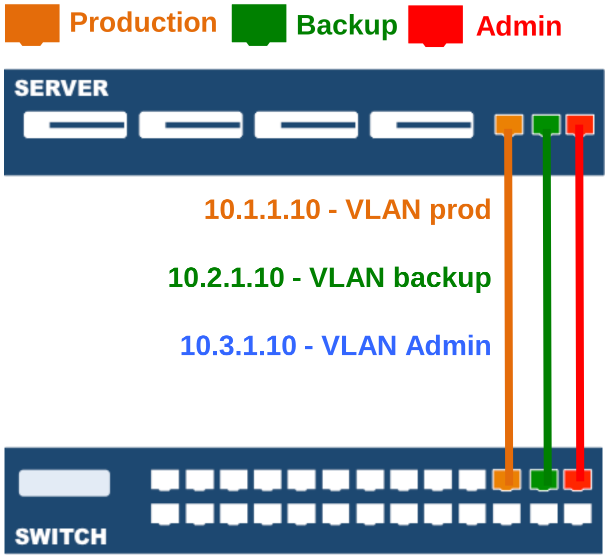
Device Manager: IT Topology Design

- **Dynamic Device Inventory**
  - Register, import or discover devices
- **Organize & Streamline Device Port Allocations**
  - Tag ports to specific purposes (Production, backup, Admin etc.)
- **Design The Network Topology**
  - Provision devices & Port Connections between devices
  - Manage device port occupancy rates
- **Unify Port, VLAN and IP Management**
- **Manage IPv6 and IPv4 dual stack allocations and transition.**
- **Advanced Reconciliation Management**
  - IPLocator Network discovery comparison with Device Manager repository

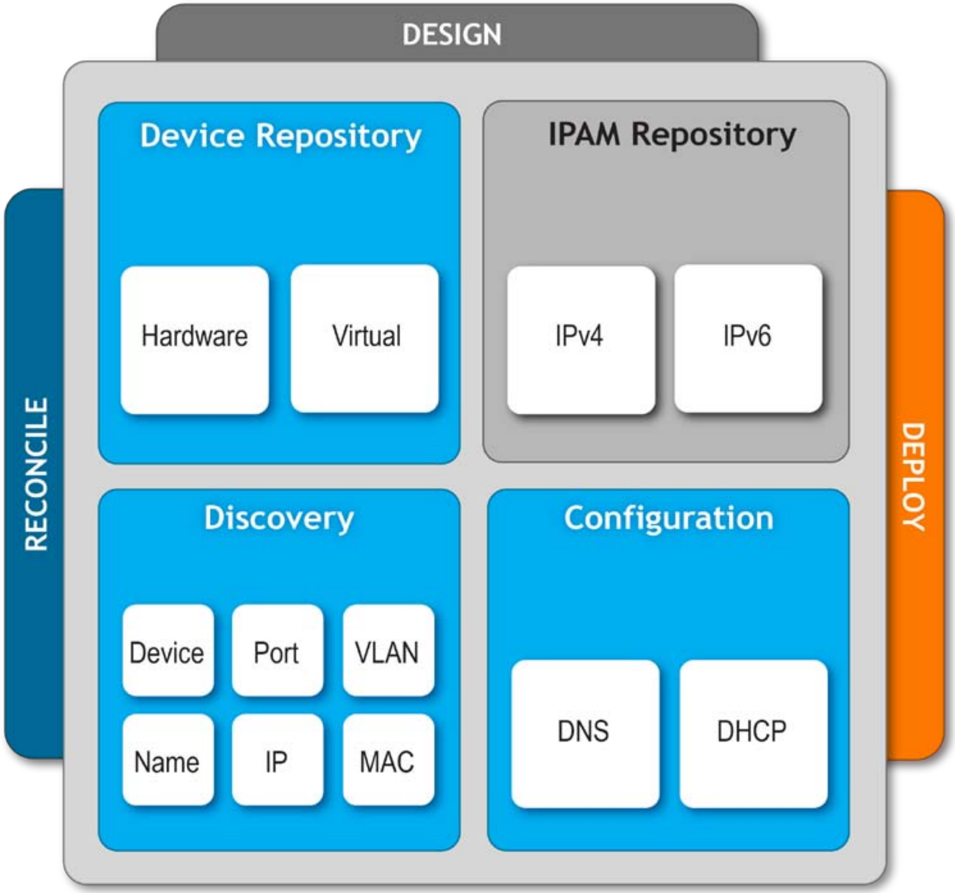
Device properties

Type, Network Interfaces, Slots, sys desc.

Metadata (location, PSU, etc.)



Smart DDI: End-to-End DDI Management



CONCLUSION

Conclusion

- **DNS-DHCP-IPAM Solutions Are the Cornerstone of Network Security Fondation**
  - Apply Security Standard with DNS & DHCP Best Practices
  - Ensure Authenticated DNS Data Exchanges with DNSSEC
  - Deploy Captive Web Portal to Control Mobile Device Access
  - Protect Against Malware with DNS Firewall
  - Manage Comprehensively IP Addresses, DNS-DHCP, VLANs and Devices

EfficientIP Company Overview

- Americas Headquarters - West Chester, Pennsylvania
- European Headquarters - Paris, France
- SmartDDI Software Company - Unified Management of DNS-DHCP-IPAM with VLAN and Devices
  - Network Design Control - Policy Driven Deployment - Process Modeling and Automation
- Coverage in 60 Plus Countries
- Doubled Number of Employees in 2012 and Again in 2013
- Solid Financial Foundation – Organic Growth & Private Funding
- Full Value Add Services: Hardware Replacement & TAC access 24x7
- Strong Technological Alliances

Microsoft CERTIFIED Partner | ISV/Software Solutions

THALES

vmware | technology alliance PARTNER

Clients

Telecommunication

Vodafone
Colt
T Mobile
SFR
Easynet
KPN
Telecom of Thailand
Qatar Telecom
Maskatel

Industries

Philips
Arkema
Ceca
Cassidian
EADS Astrium
EDF
GDF SUEZ
Globalia
Salomon
AtomiC
Universal Music Group
Japan Tobacco
Tallgrass

Banks & Insurances

Coface
BRED
Axa Wealth
Credit Agricole
Zurich Financial Services
Bank of France
Henner Group

Transports

Norbert Dentressangle
SANEF
APRR
Metro of Madrid
Metro of Paris

Services

3Suisses
CEA
La Poste
Sopra Group

THANK YOU FOR YOUR ATTENTION!