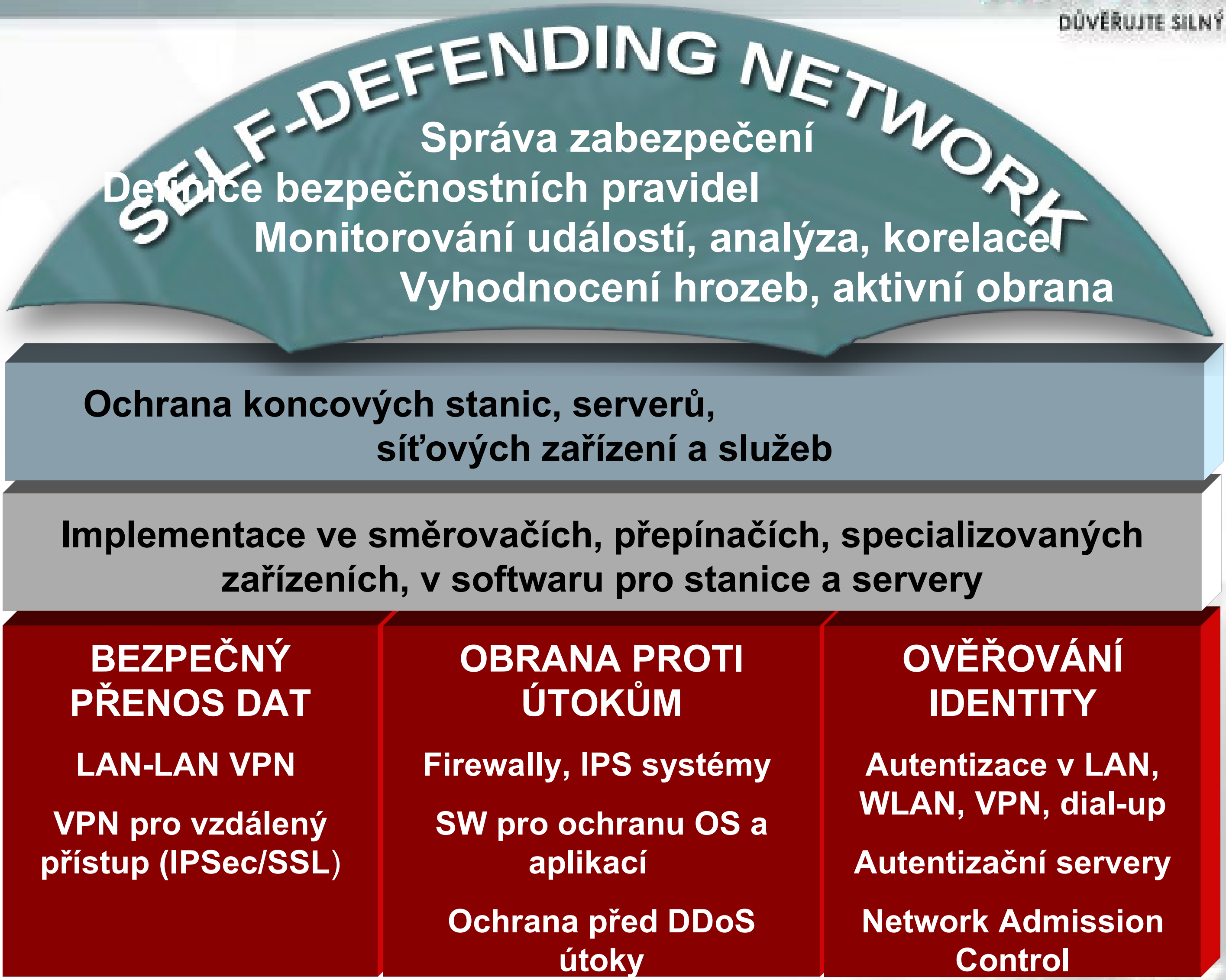
ALEF NULA

DŮVĚŘUJTE SILNÝM

Bezpečnostní řešení

Martin Biško
martin.bisko@alefnula.com

Cisco Self-Defending Network



Správa zabezpečení

Definice bezpečnostních pravidel

Monitorování událostí, analýza, korelace

Vyhodnocení hrozeb, aktivní obrana

Ochrana koncových stanic, serverů, síťových zařízení a služeb

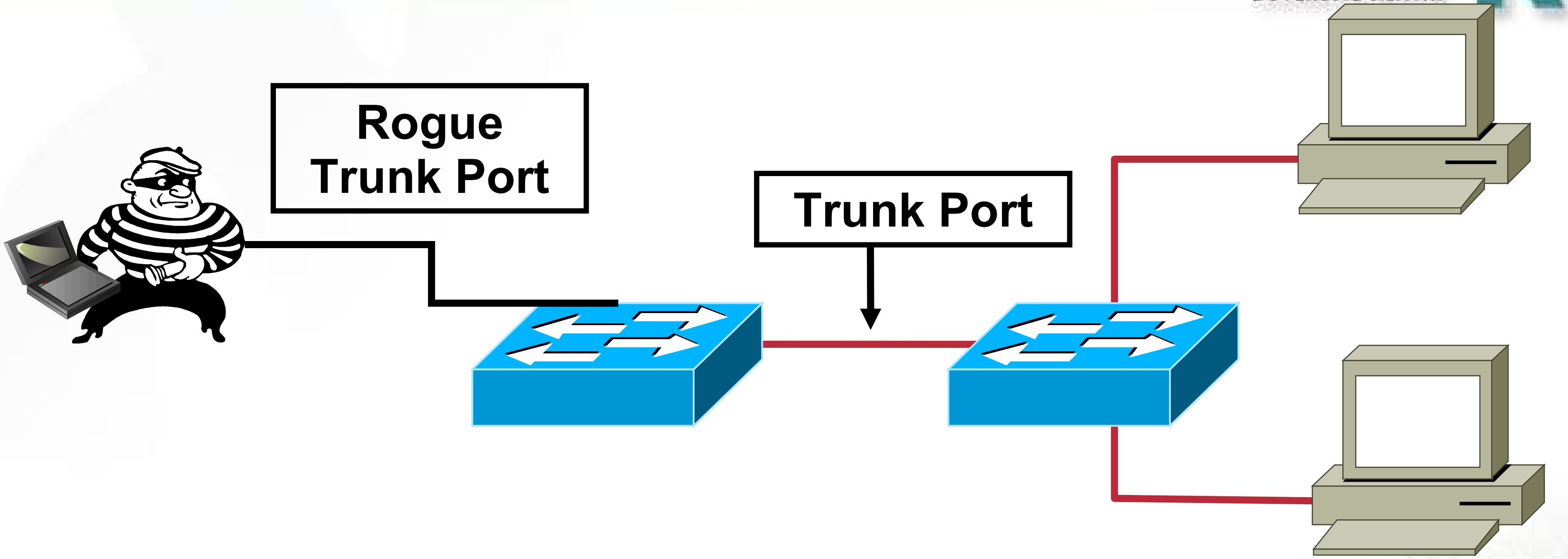
Implementace ve směrovačích, přepínačích, specializovaných zařízeních, v softwaru pro stanice a servery

BEZPEČNÝ PŘENOS DAT	OBRANA PROTI ÚTOKŮM	OVĚŘOVÁNÍ IDENTITY
LAN-LAN VPN VPN pro vzdálený přístup (IPSec/SSL)	Firewally, IPS systémy SW pro ochranu OS a aplikací Ochrana před DDoS útoky	Autentizace v LAN, WLAN, VPN, dial-up Autentizační servery Network Admission Control

ALEF NULA
DŮVĚŘUJTE SILNÝM

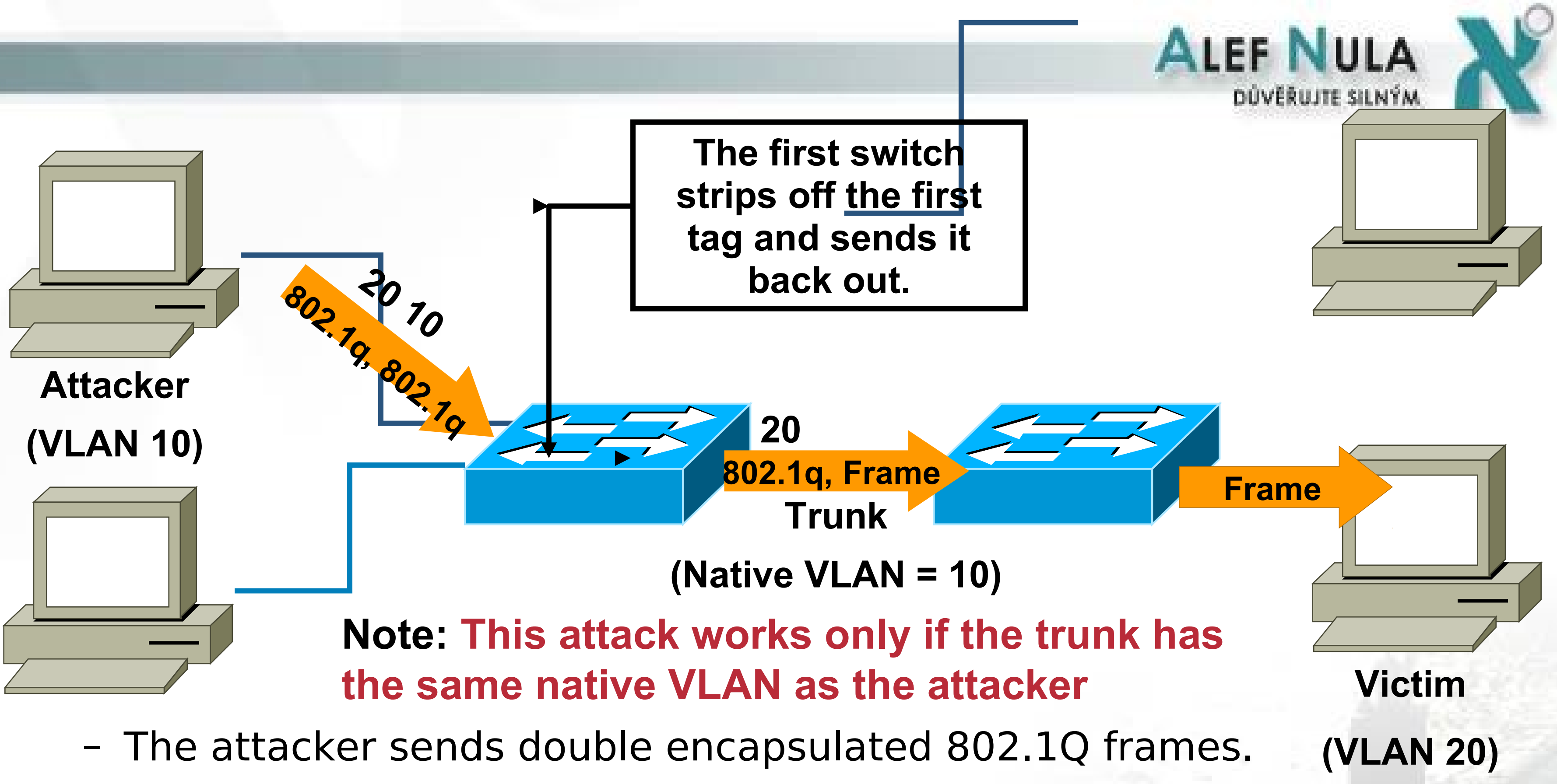
LAN Security

VLAN Hopping by Switch Spoofing



- An attacker tricks a network switch into believing it is a legitimate switch on the network needing trunking.
- Autotrunking allows the rogue station to become a member of all VLANs.

VLAN Hopping by Double Tagging



The first switch strips off the first tag and sends it back out.

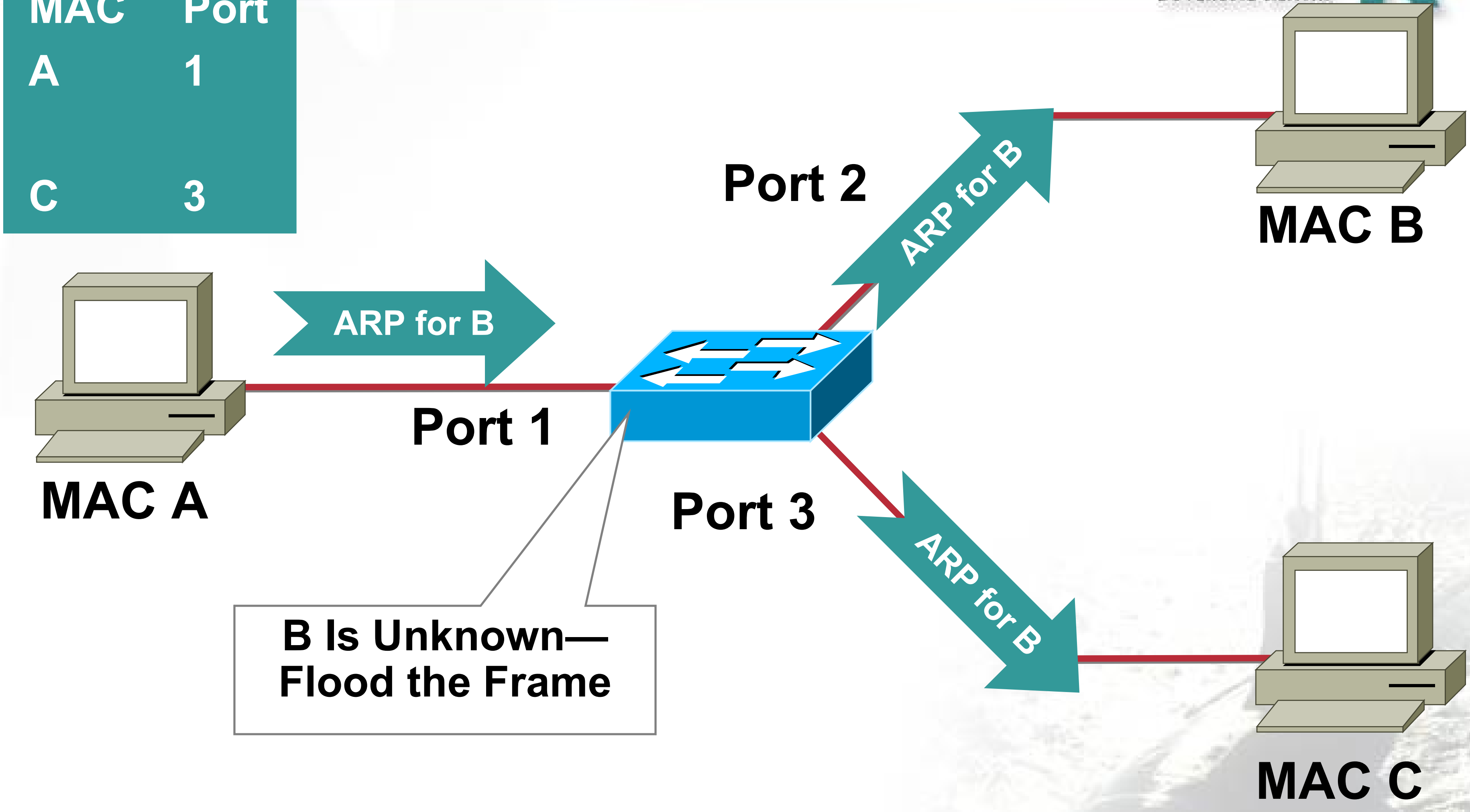
Note: **This attack works only if the trunk has the same native VLAN as the attacker**

- The attacker sends double encapsulated 802.1Q frames.
- The switch performs only one level of decapsulation.
- Only unidirectional traffic is passed.
- It works even if the trunk ports are set to off.

MAC Attacks

Normal CAM Behavior 1/3

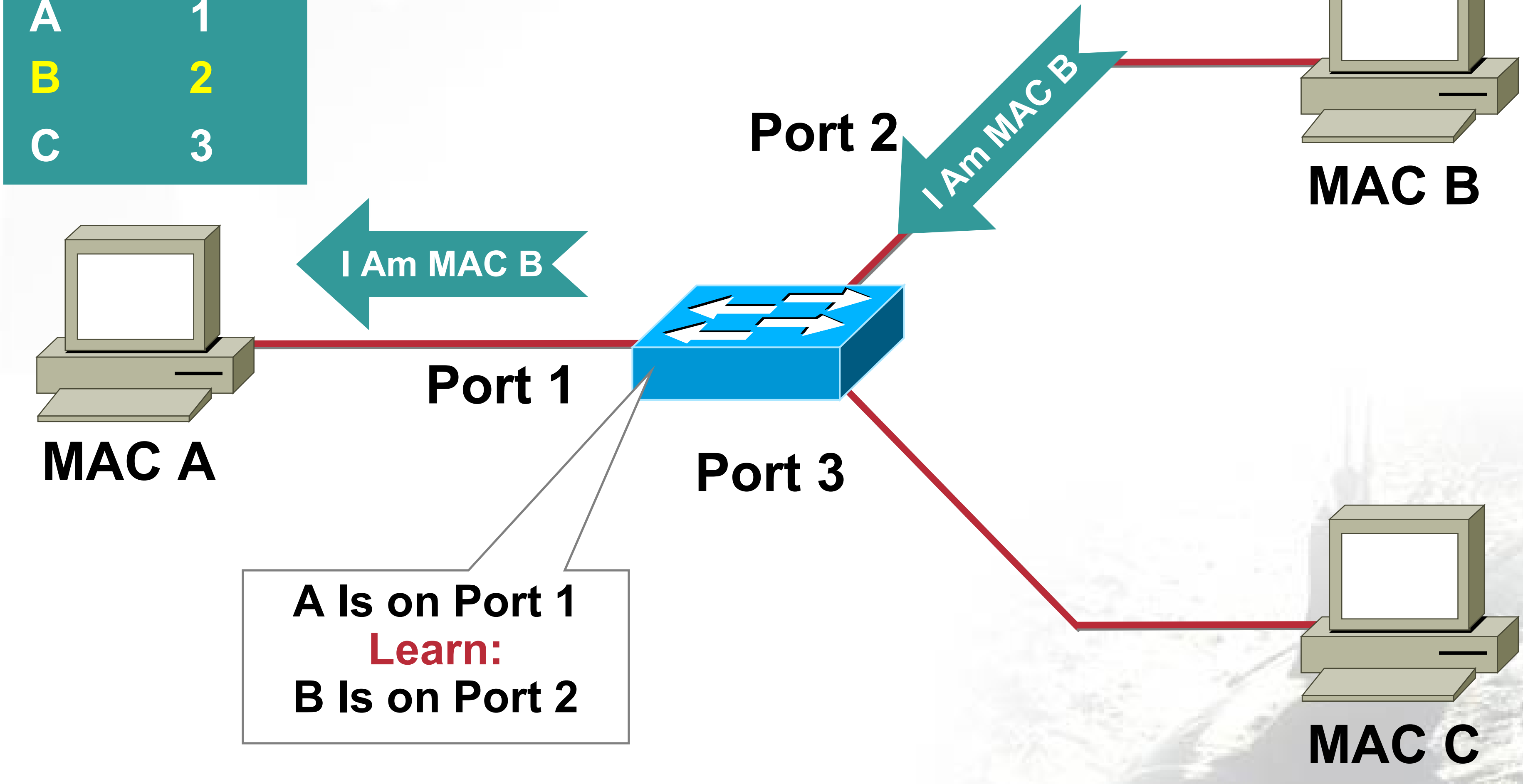
MAC	Port
A	1
C	3



B Is Unknown—
Flood the Frame

Normal CAM Behavior 2/3

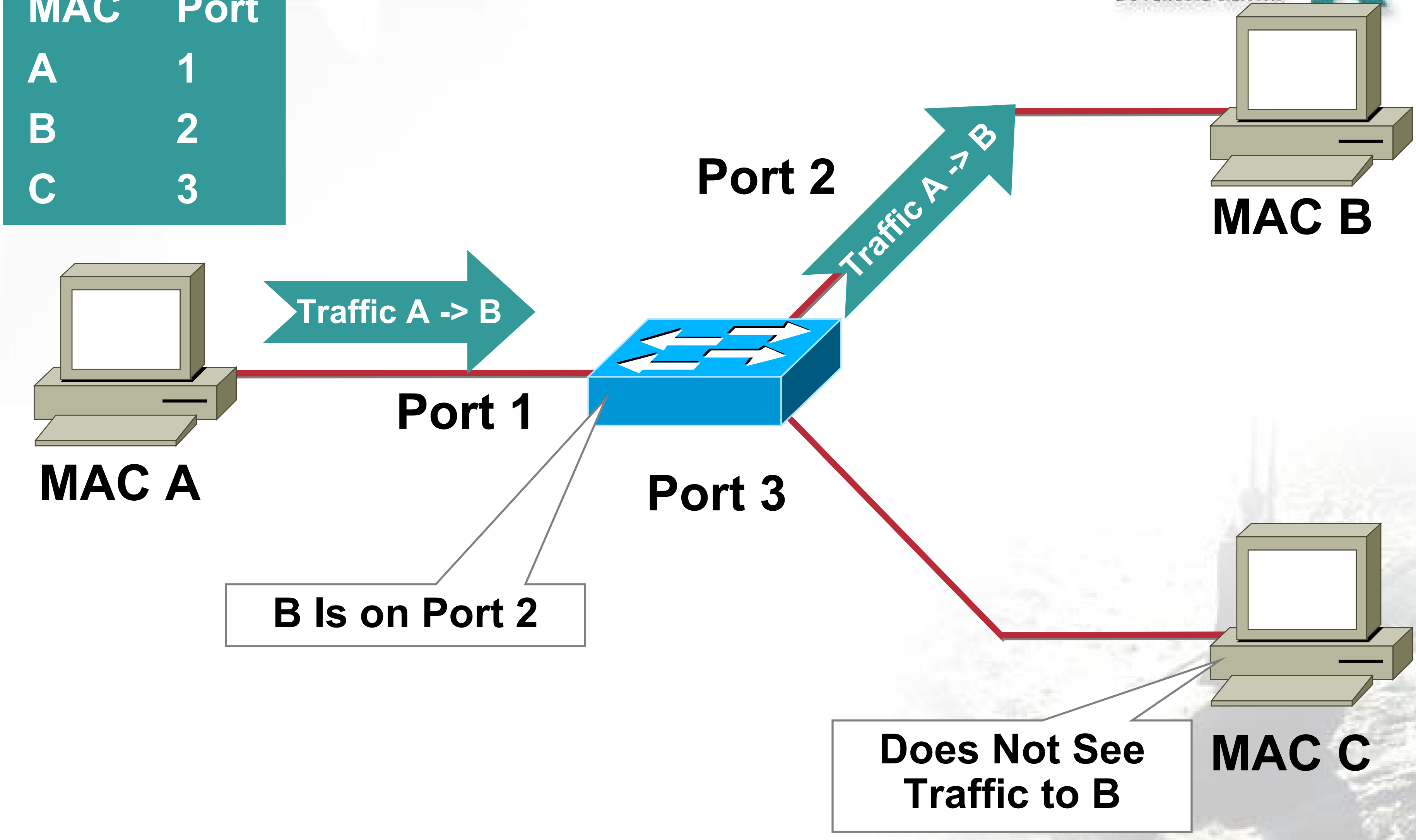
MAC	Port
A	1
B	2
C	3



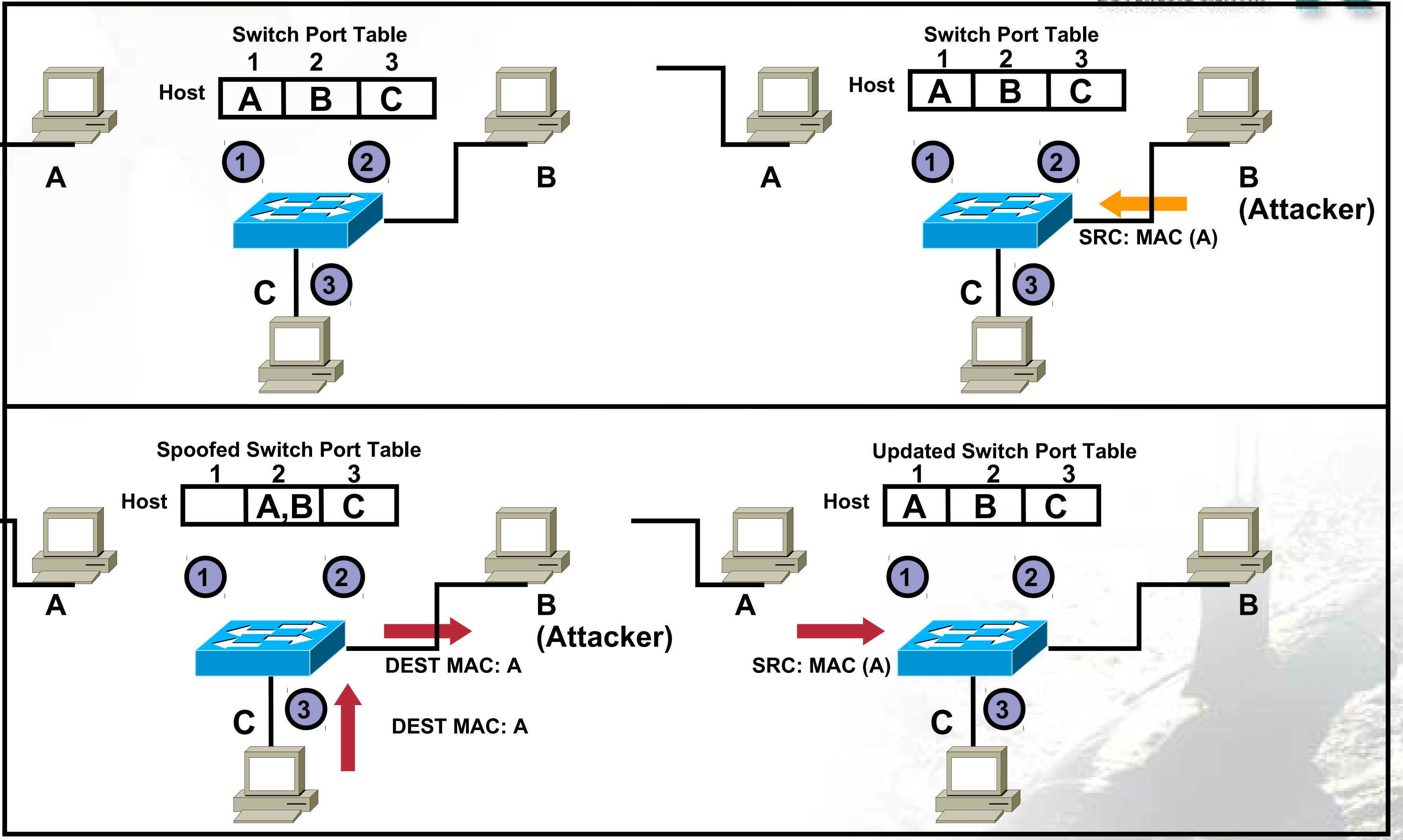
A Is on Port 1
Learn:
B Is on Port 2

Normal CAM Behavior 3/3

MAC	Port
A	1
B	2
C	3



MAC Address Spoofing Attack



Switch Port Table

	1	2	3
Host	A	B	C

Switch Port Table

	1	2	3
Host	A	B	C

Spoofed Switch Port Table

	1	2	3
Host		A,B	C

Updated Switch Port Table

	1	2	3
Host	A	B	C

www.alefnula.com

Port Security

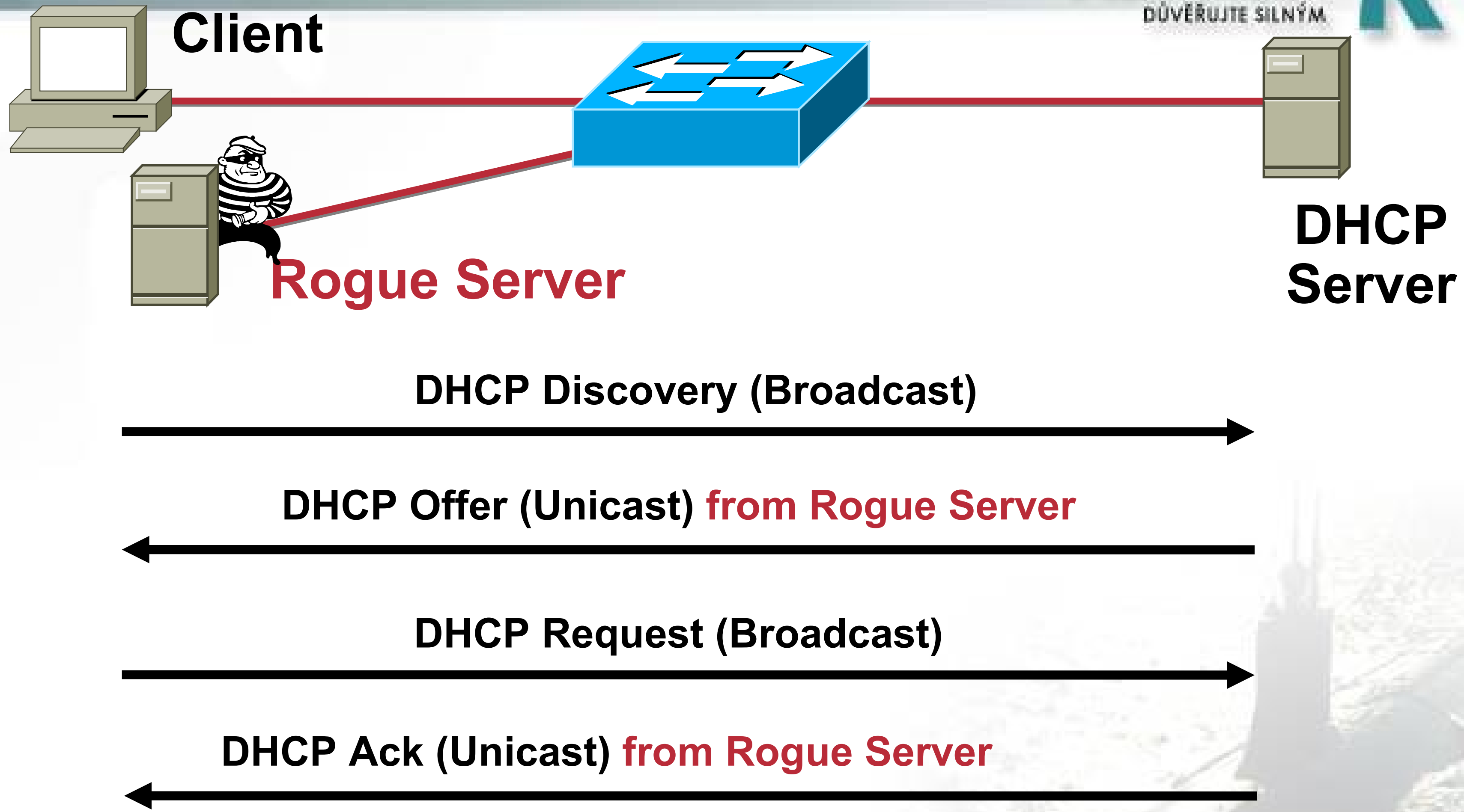
Not All Port Security Created Equal

- In the past you would have to type in the ONLY MAC you were going to allow on that port
- You can now put a limit to how many MAC address a port will learn
- You can also put timers in to state how long the MAC address will be bound to that switch port
- You might still want to do static MAC entries on ports that there should be no movement of devices, as in server farms
- If you are going to be running Cisco IPT, you will need a minimum of three MAC addresses on each port if you are running voice VLANs
- New feature called “Sticky Port Security”, settings will survive reboot (not on all switches)

ALEF NULA
DŮVĚŘUJTE SILNÝM

DHCP Attacks

DHCP Attack Types
Rogue DHCP Server Attack



Client

Rogue Server

DHCP Server

DHCP Discovery (Broadcast)

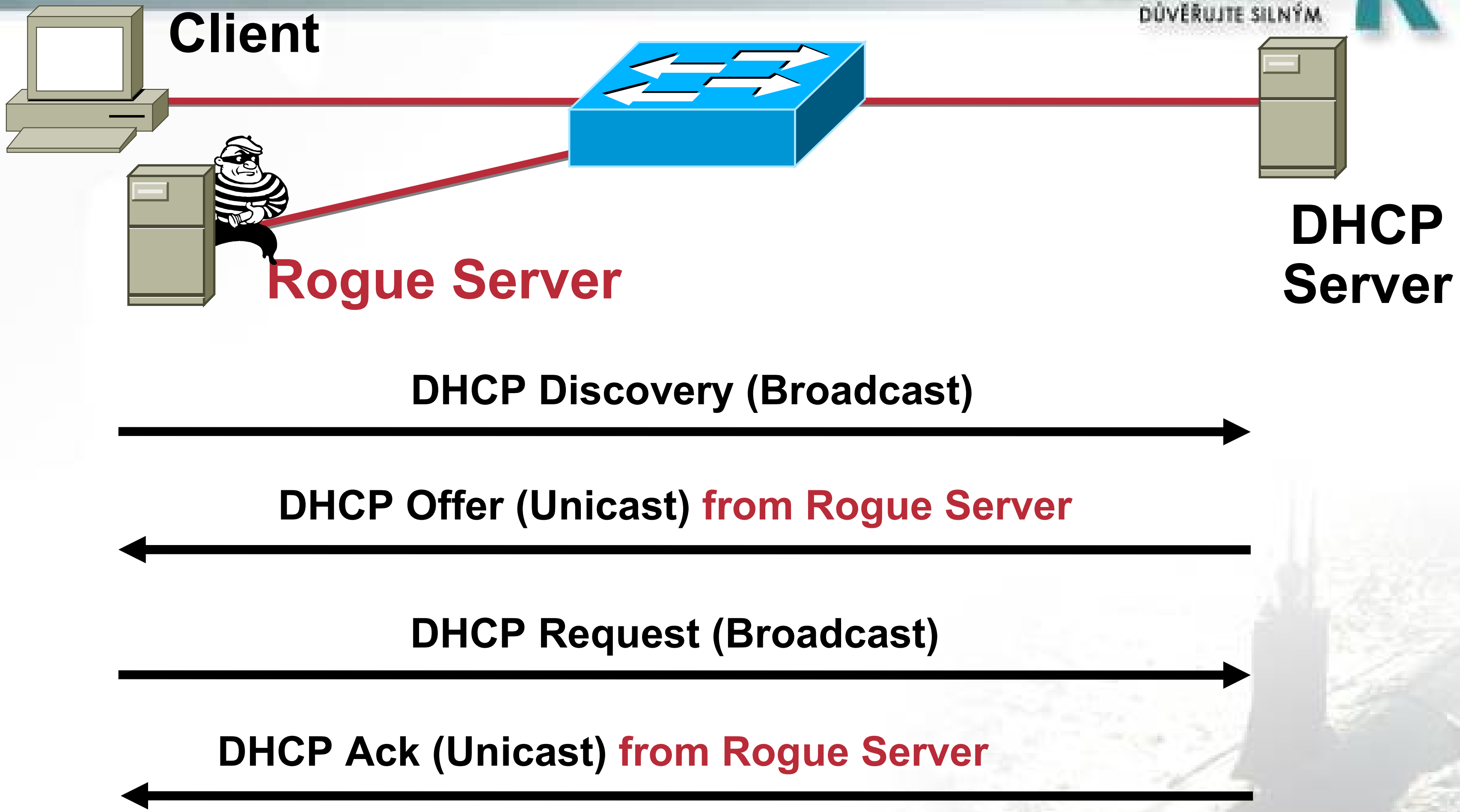
DHCP Offer (Unicast) from Rogue Server

DHCP Request (Broadcast)

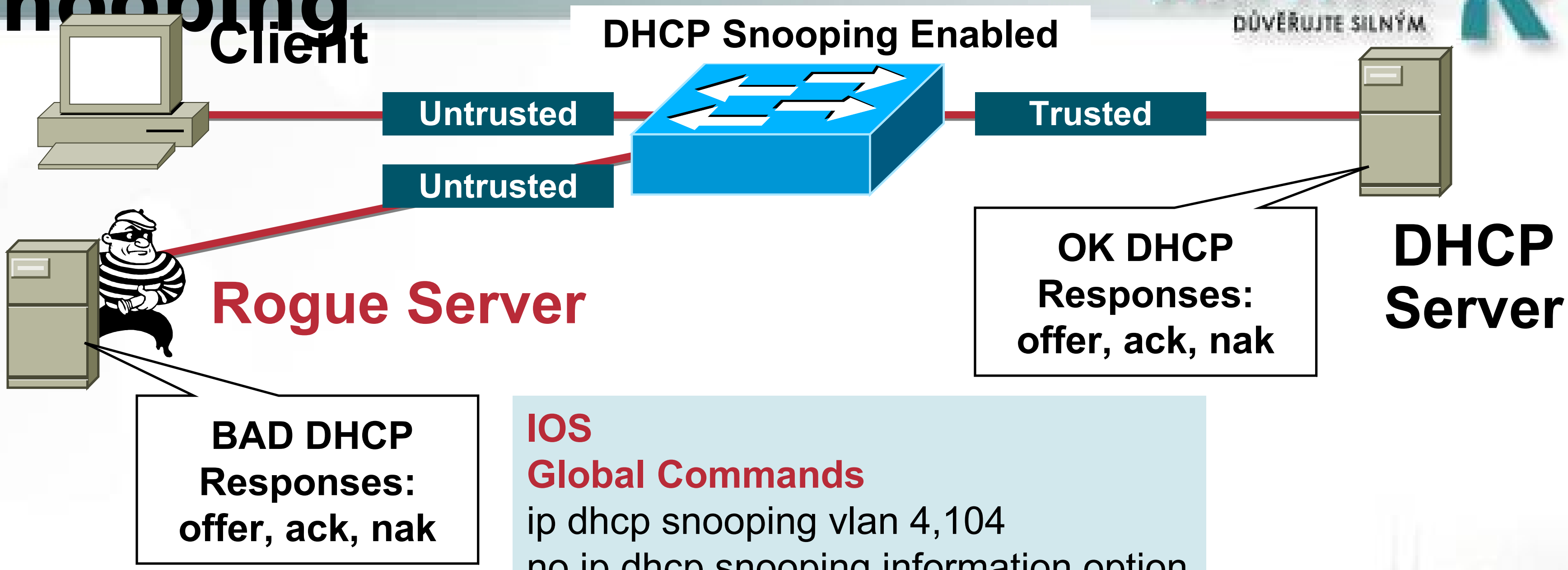
DHCP Ack (Unicast) from Rogue Server

www.alefnula.com

DHCP Attack Types
Rogue DHCP Server Attack


Client
Rogue Server
DHCP Server
DHCP Discovery (Broadcast)
DHCP Offer (Unicast) from Rogue Server
DHCP Request (Broadcast)
DHCP Ack (Unicast) from Rogue Server

Countermeasures for DHCP Attacks Rogue DHCP Server = DHCP Snooping



IOS
Global Commands

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

DHCP Snooping Untrusted Client

Interface Commands

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
```

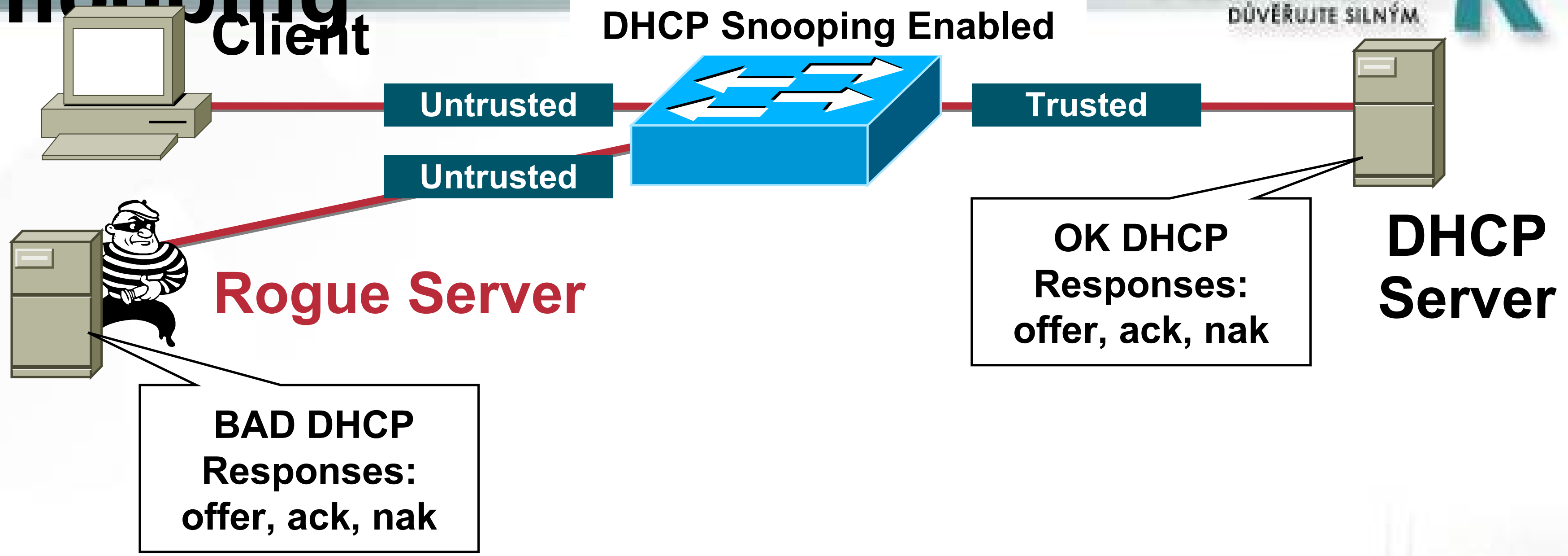
DHCP Snooping Trusted Server or Uplink

Interface Commands

```
ip dhcp snooping trust
```

- By default all ports in the VLAN are untrusted

Countermeasures for DHCP Attacks Rogue DHCP Server = DHCP Snooping



Client

DHCP Snooping Enabled

Untrusted

Untrusted

Trusted

Rogue Server

DHCP Server

OK DHCP Responses: offer, ack, nak

BAD DHCP Responses: offer, ack, nak

DHCP Snooping Binding Table

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
```

- Table is built by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires

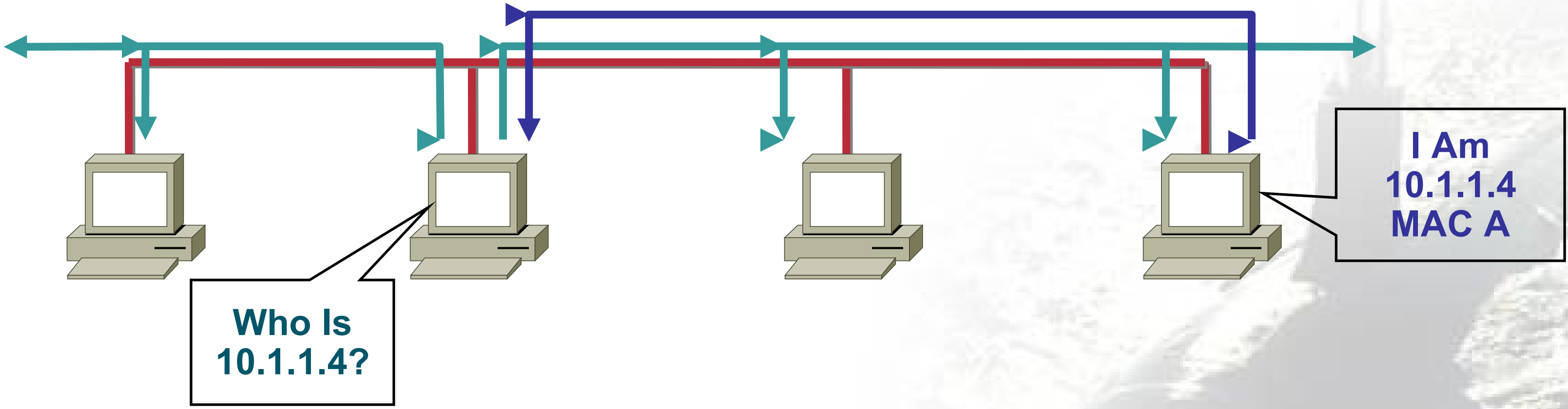
ALEF NULA

DŮVĚŘUJTE SILNÝM

ARP Attacks

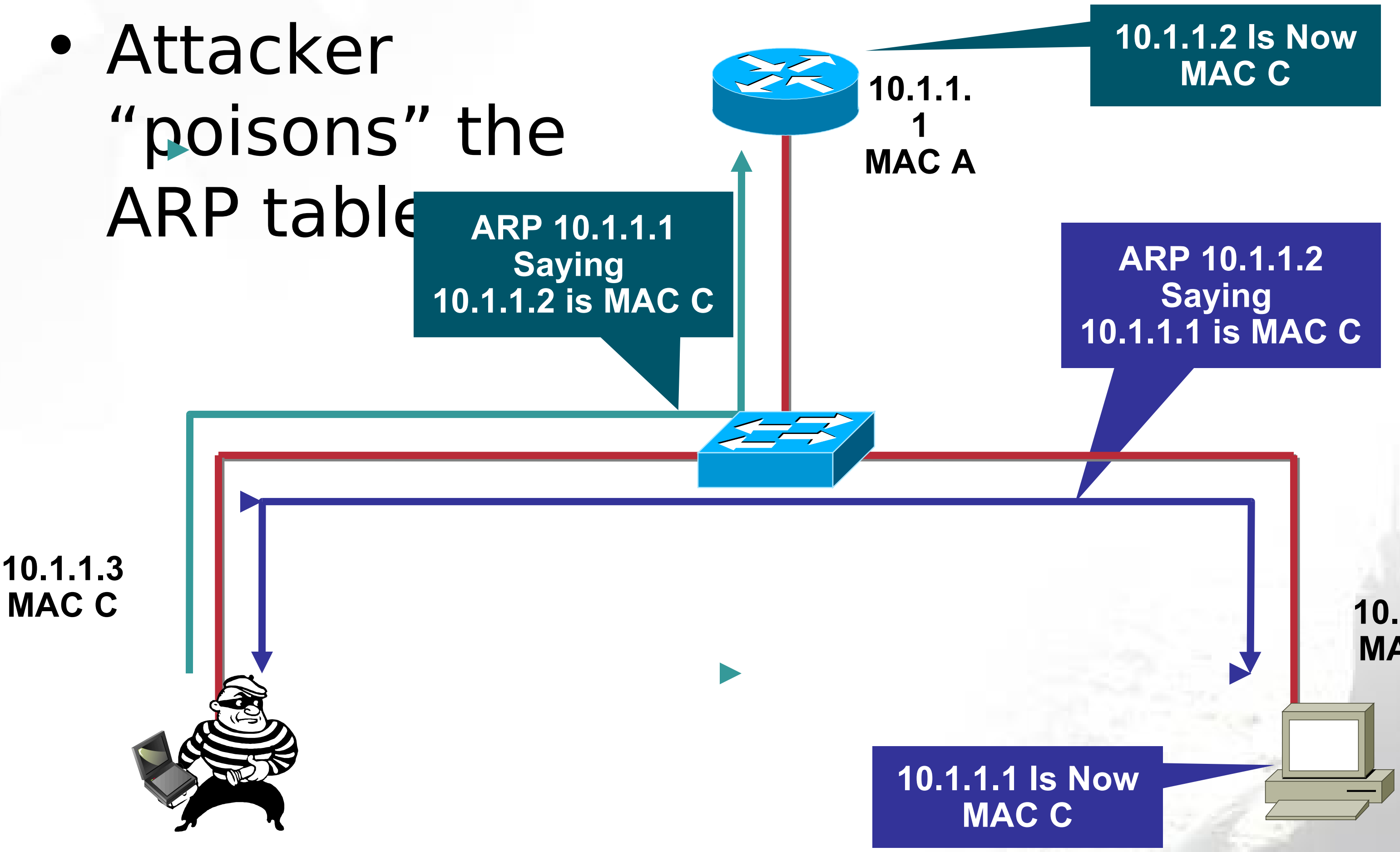
ARP Function Review

- Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address
  - This ARP request is broadcast using protocol 0806
- All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply



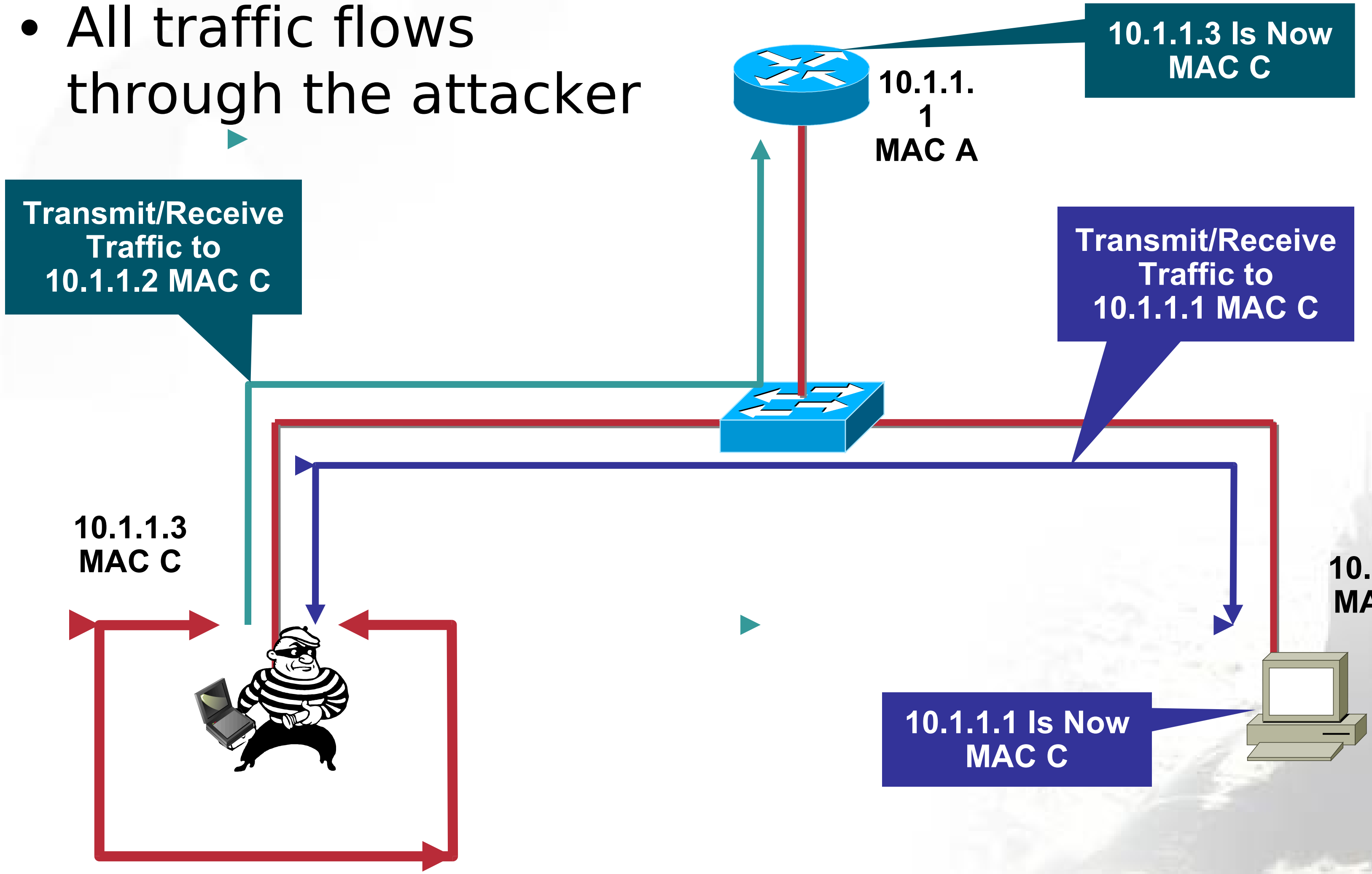
ARP Attack in Action

- Attacker “poisons” the ARP table

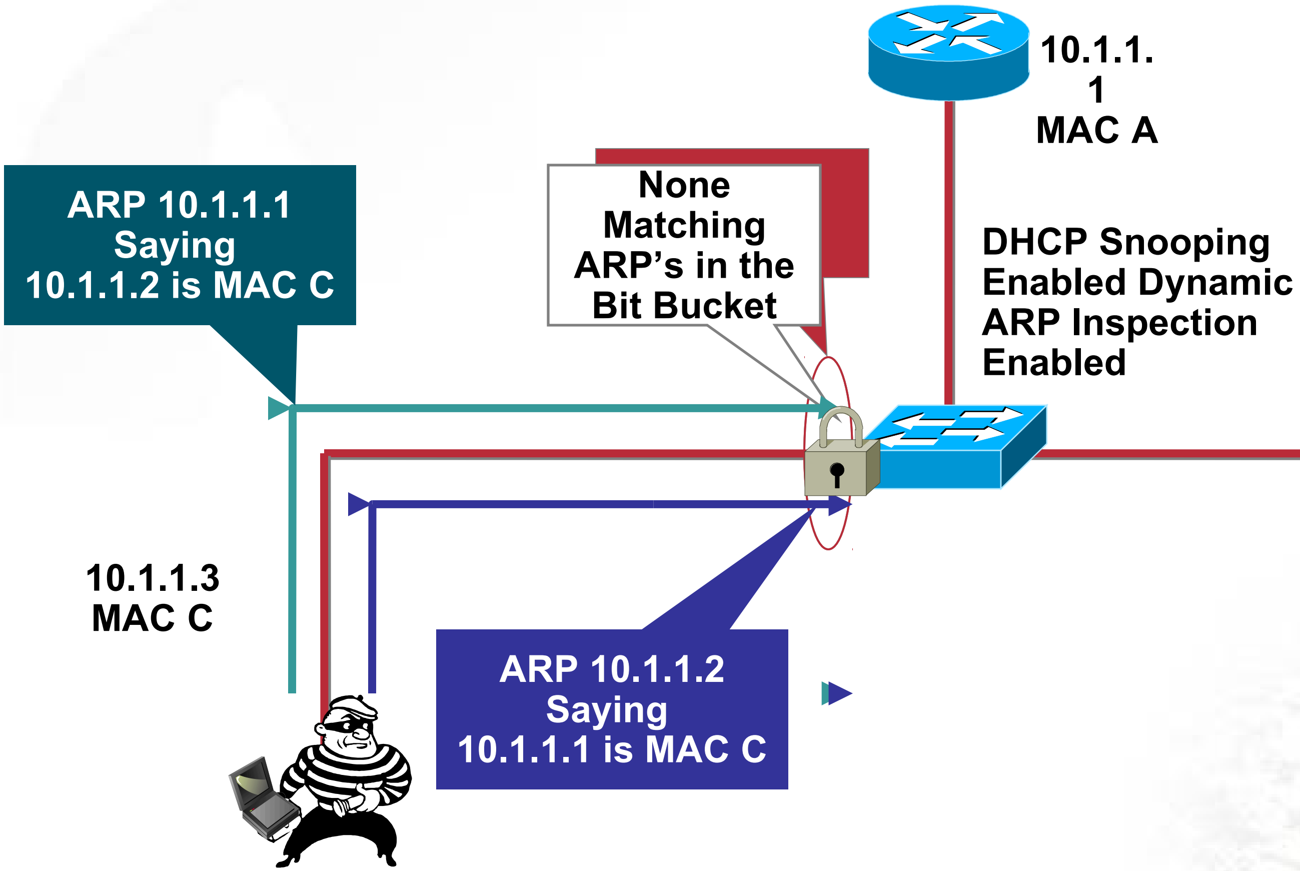


ARP Attack in Action

- All traffic flows through the attacker


10.1.1.3 Is Now MAC C
10.1.1.
1
MAC A
Transmit/Receive Traffic to 10.1.1.2 MAC C
Transmit/Receive Traffic to 10.1.1.1 MAC C
10.1.1.3
MAC C
10.1.1.2
MAC B
10.1.1.1 Is Now MAC C

Countermeasures to ARP Attacks: Dynamic ARP Inspection



- Uses the DHCP Snooping Binding table information
- Dynamic ARP Inspection
  - All ARP packets must match the IP/MAC Binding table entries
  - If the entries do not match, throw them in the bit bucket

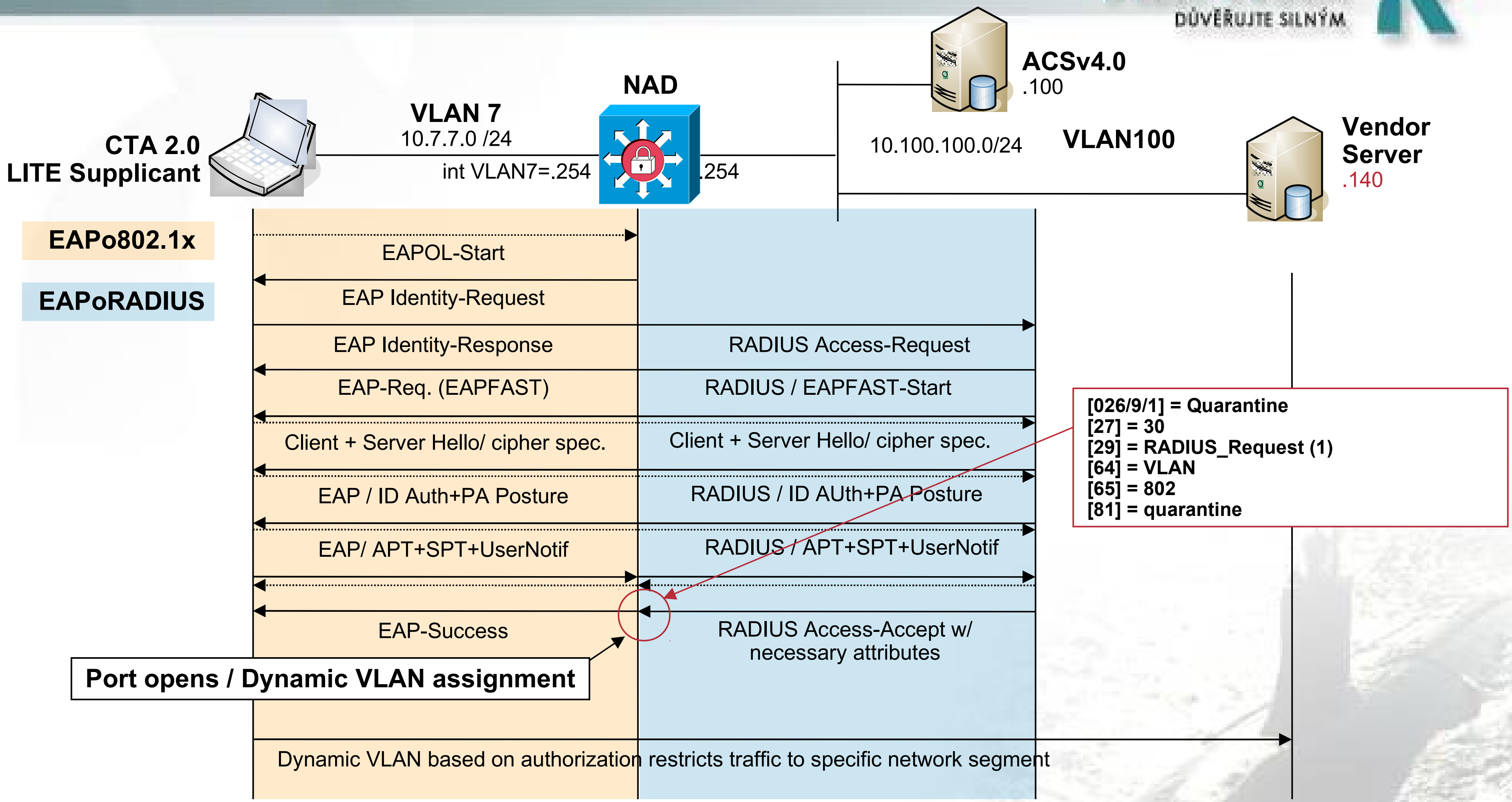
ALEF NULA
DŮVĚŘUJTE SILNÝM

Network Admission Control

NAC-L2-802.1x:
Identity and Posture

Key:

[26/9/1]	cisco-av-pair
[27]	Session-Timeout
[29]	Termination-Action
[64]	Tunnel-type
[65]	Tunnel-Medium-Type
[81]	Tunnel-Private-Group-ID



EAPOL-Start

EAP Identity-Request

EAP Identity-Response — RADIUS Access-Request

EAP-Req. (EAPFAST) — RADIUS / EAPFAST-Start

Client + Server Hello/ cipher spec. — Client + Server Hello/ cipher spec.

EAP / ID Auth+PA Posture — RADIUS / ID AUth+PA Posture

EAP/ APT+SPT+UserNotif — RADIUS / APT+SPT+UserNotif

EAP-Success — RADIUS Access-Accept w/ necessary attributes

[026/9/1] = Quarantine
[27] = 30
[29] = RADIUS_Request (1)
[64] = VLAN
[65] = 802
[81] = quarantine

Port opens / Dynamic VLAN assignment

Dynamic VLAN based on authorization restricts traffic to specific network segment

NAC-L2-802.1x assume that ACLs pre-exist on the device

ALEF NULA
DŮVĚŘUJTE SILNÝM

IPS SOLUTIONS

Types of IDS/IPS Systems

Signature based

- e.g. more than 100 ICMP packets/minute

Policy based

- e.g. deny all UDP packets

Anomaly based

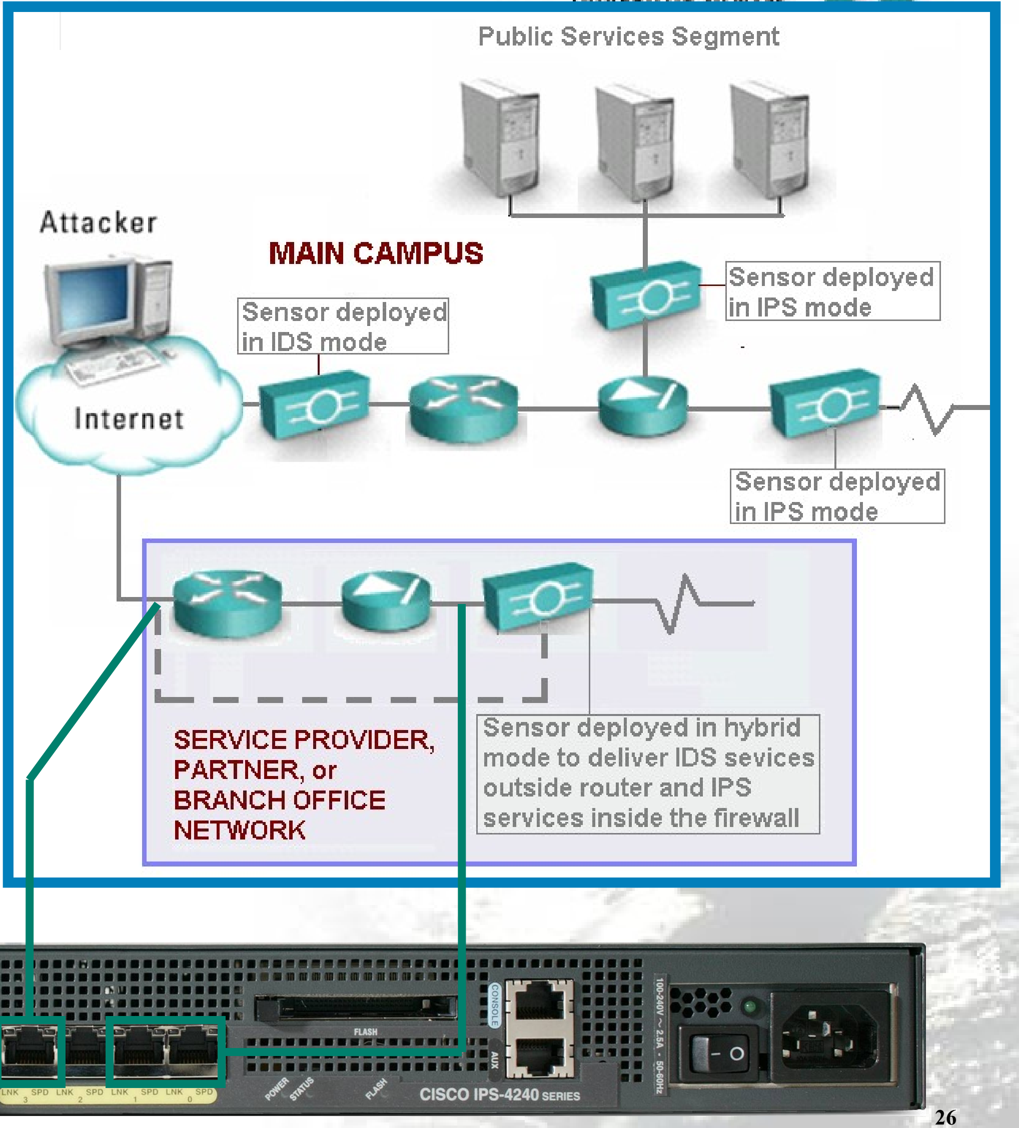
- e.g. packet contains invalid protocol options

Network or Host based

- HIDS/NIDS and HIPS/NIPS

Cisco IPS Software v6.x

Hybrid IDS & IPS services allow a single device to be deployed in IDS mode at the network edge and simultaneously in the IPS mode to stop worms identified internally



Public Services Segment
Attacker
Internet
MAIN CAMPUS
Sensor deployed in IDS mode
Sensor deployed in IPS mode
Sensor deployed in IPS mode
SERVICE PROVIDER, PARTNER, or BRANCH OFFICE NETWORK
Sensor deployed in hybrid mode to deliver IDS sevices outside router and IPS services inside the firewall
MGMT
USB2 USB1
LNK SPD LNK SPD LNK SPD LNK SPD
3 2 1 0
FLASH
CONSOLE
AUX
POWER
STATUS
FLASH
CISCO IPS-4240 SERIES
100-240V ~ 2.5A 50-60Hz

Comparing IDS and IPS Solutions

	Advantages	Disadvantages
IDS (Promiscuous mode)	• No impact on network (latency, jitter) • No impact on sensor failure • No network impact on sensor overload	• Response action cannot stop trigger packets • Correct tuning required for response actions • More vulnerable to network evasion techniques
IPS (In-line mode)	• Trigger packets stopped • Can use stream normalization techniques	• Sensor issues might affect network traffic • Sensor overloading impacts network • Some impact on network (latency, jitter)

Cisco IPS Software v6.x

Expanded Mitigation Actions to STOP Attacks

Drop Actions for comprehensive mitigation

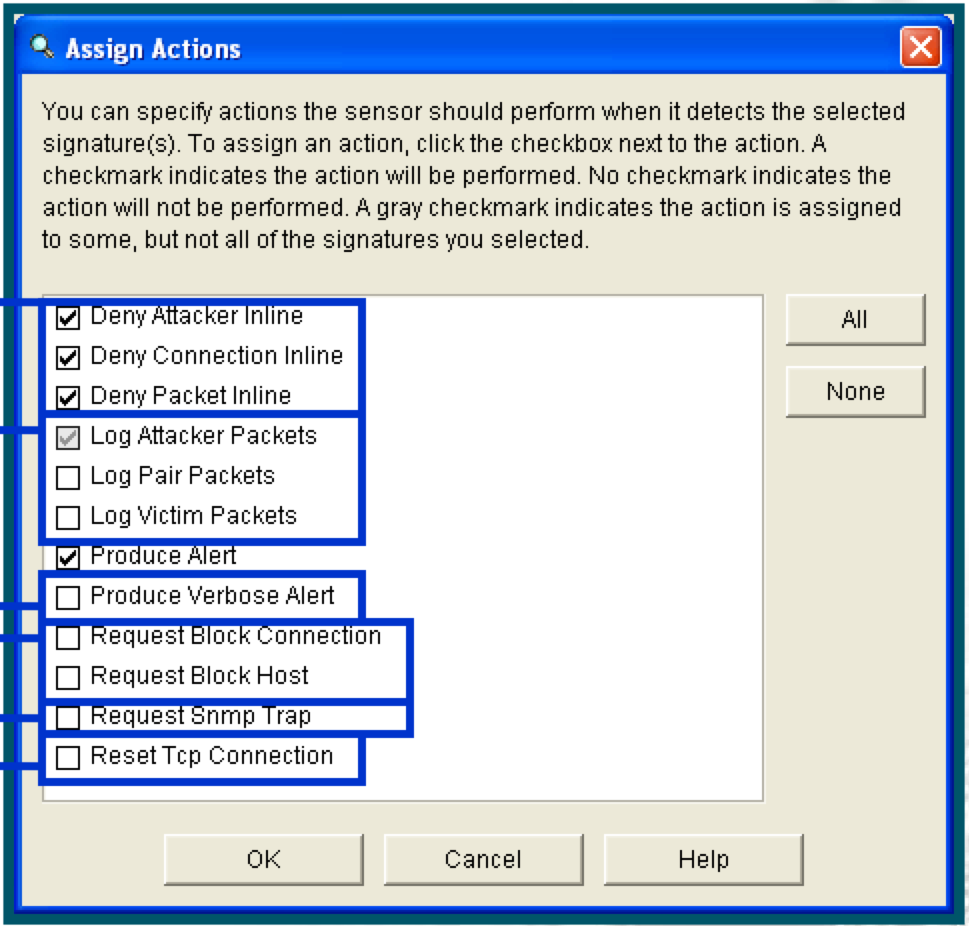
et Logging for advanced forensics sis

sion of Trigger Packet in alarm for er visibility into attack

Blocking hosts at strategic network ingress points

Trap generation with alarm s and sensor diagnostics

ection resets to mitigate TCP d attacks

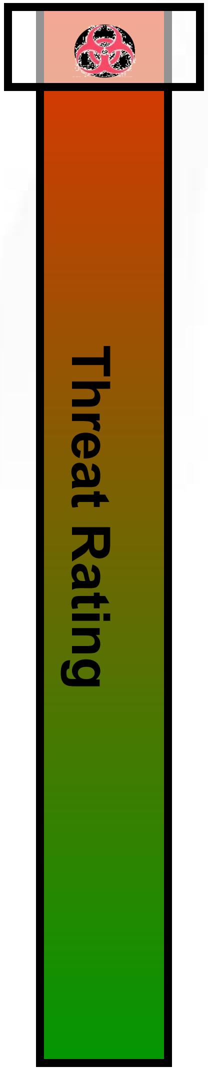


Assign Actions

You can specify actions the sensor should perform when it detects the selected signature(s). To assign an action, click the checkbox next to the action. A checkmark indicates the action will be performed. No checkmark indicates the action will not be performed. A gray checkmark indicates the action is assigned to some, but not all of the signatures you selected.

☑ Deny Attacker Inline
☑ Deny Connection Inline
☑ Deny Packet Inline
☑ Log Attacker Packets
□ Log Pair Packets
□ Log Victim Packets
☑ Produce Alert
□ Produce Verbose Alert
□ Request Block Connection
□ Request Block Host
□ Request Snmp Trap
□ Reset Tcp Connection

Cisco IPS Overview:
Risk-Management-based Security Policy



Event Severity — How urgent is the threat?

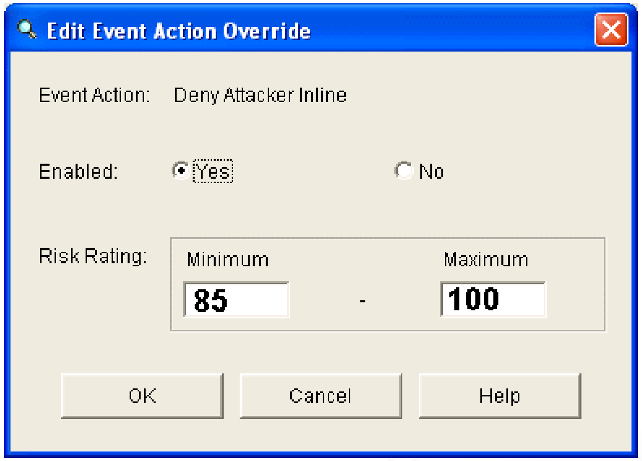
+ **Signature Fidelity** — How Prone to false positive?

+ **Attack Relevancy** — Is attack relevant to host being attacked?

+ **Asset Value of Target** — How critical is this destination host?

= Risk Rating

Drives Mitigation Policy



Event Action: Deny Attacker Inline

Enabled: ● Yes ○ No

Risk Rating: Minimum 85 - Maximum 100

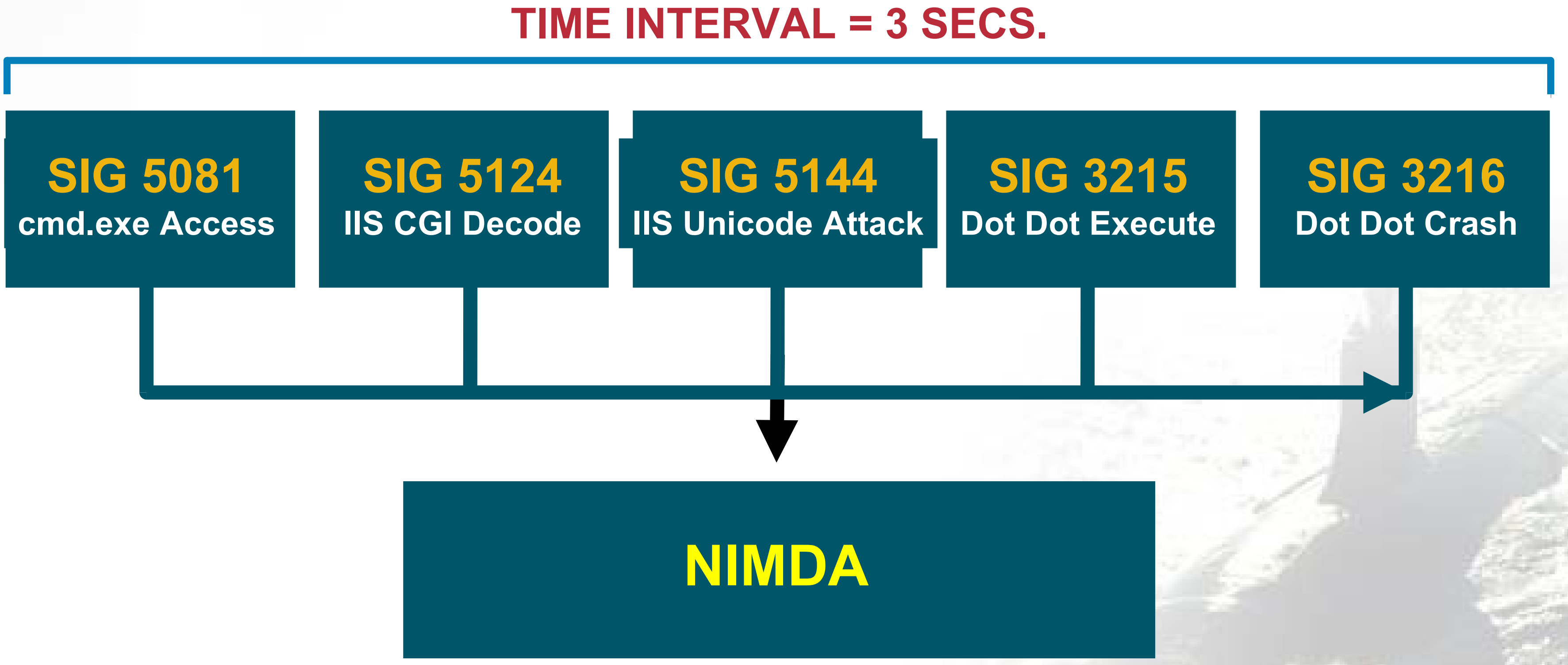
Customizable Risk Rating Thresholds :

0 < RR < 35	Alarm
35 < RR < 85	Alarm & Log Packets
85 < RR < 100	Drop Packet

Result: Calibrated Risk Rating enables scalable management of sophisticated threat prevention technologies

Process for Accurate Threat Mitigation:
Integrated Event Correlation

If SIG IDs 5081, 5124, 5114, 3215 & 3216 Fire within a 3 Sec. Interval, then Trigger the Meta Event, “Nimda”



TIME INTERVAL = 3 SECS.

SIG 5081
cmd.exe Access

SIG 5124
IIS CGI Decode

SIG 5144
IIS Unicode Attack

SIG 3215
Dot Dot Execute

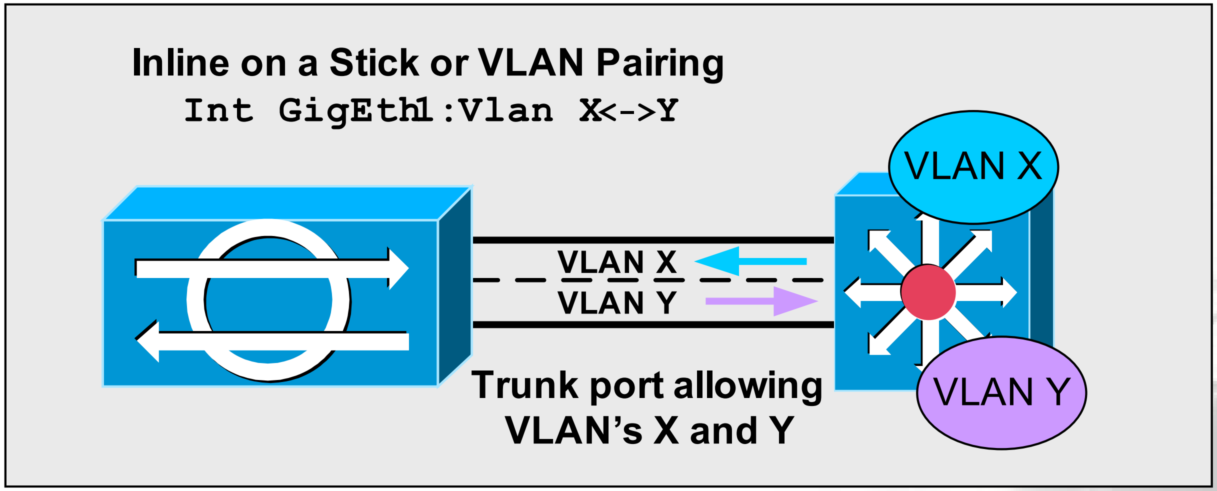
SIG 3216
Dot Dot Crash

NIMDA

IPS Version 5.1

Deployment flexibility via Inline-on-a-Stick

- VLAN pairing allows a sensor to bridge VLANs together on the same physical interface by defining, in practice, sub-interfaces that tell the sensor to bring packets in on VLAN X and out on VLAN Y
- VLAN header information is rewritten by the sensor on each VLAN pair
- Not tested to work with non-Cisco or EoS switches


Inline on a Stick or VLAN Pairing
Int GigEth1:Vlan X<->Y
VLAN X
VLAN X
VLAN Y
VLAN Y
Trunk port allowing VLAN's X and Y

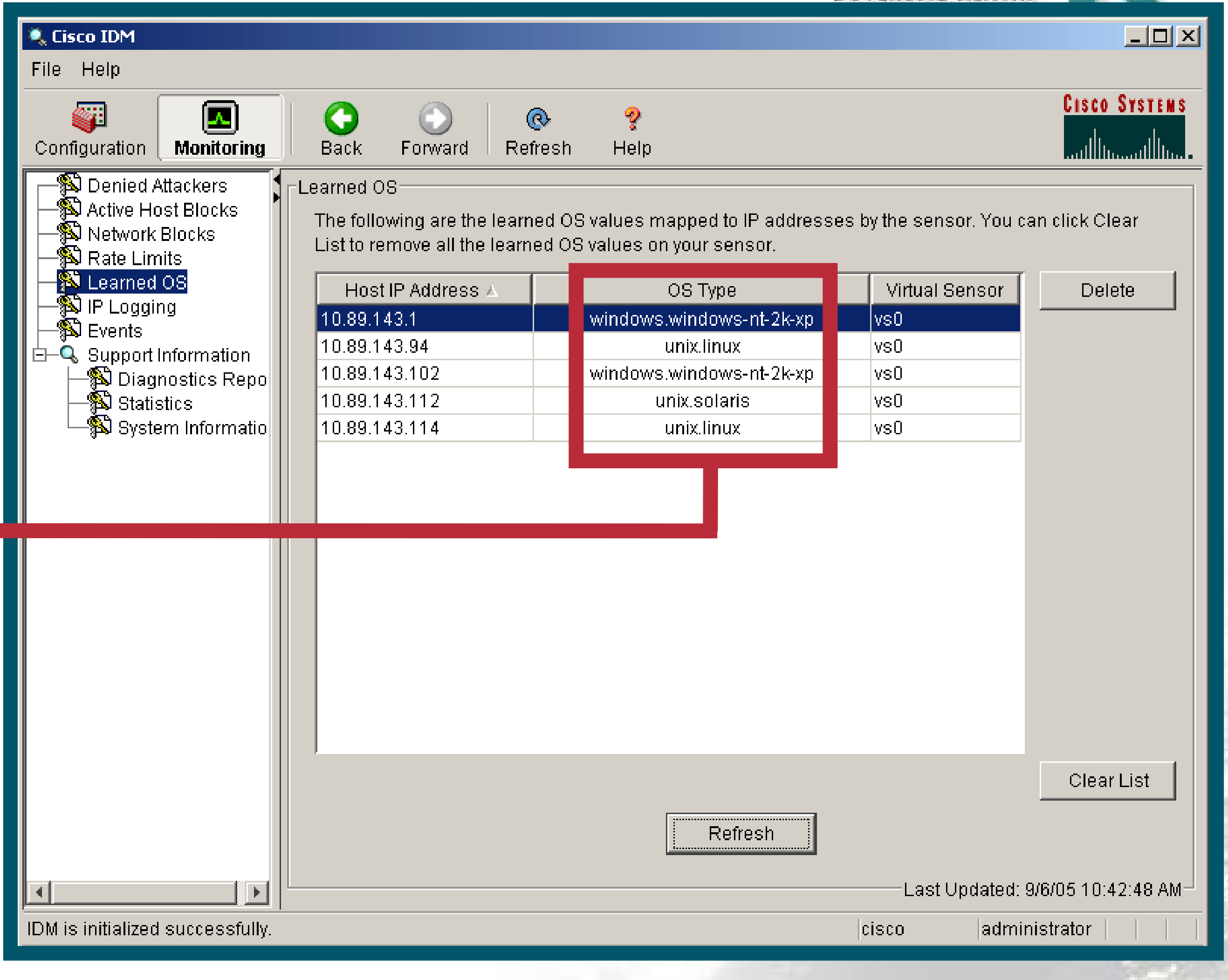
IPS Version 6.0

CTR Integration – OS Identification

IP Address of Endpoint

Learned OS of target system

Virtual Context on which alarm was triggered



Learned OS

The following are the learned OS values mapped to IP addresses by the sensor. You can click Clear List to remove all the learned OS values on your sensor.

Host IP Address	OS Type	Virtual Sensor
10.89.143.1	windows.windows-nt-2k-xp	vs0
10.89.143.94	unix.linux	vs0
10.89.143.102	windows.windows-nt-2k-xp	vs0
10.89.143.112	unix.solaris	vs0
10.89.143.114	unix.linux	vs0

Last Updated: 9/6/05 10:42:48 AM

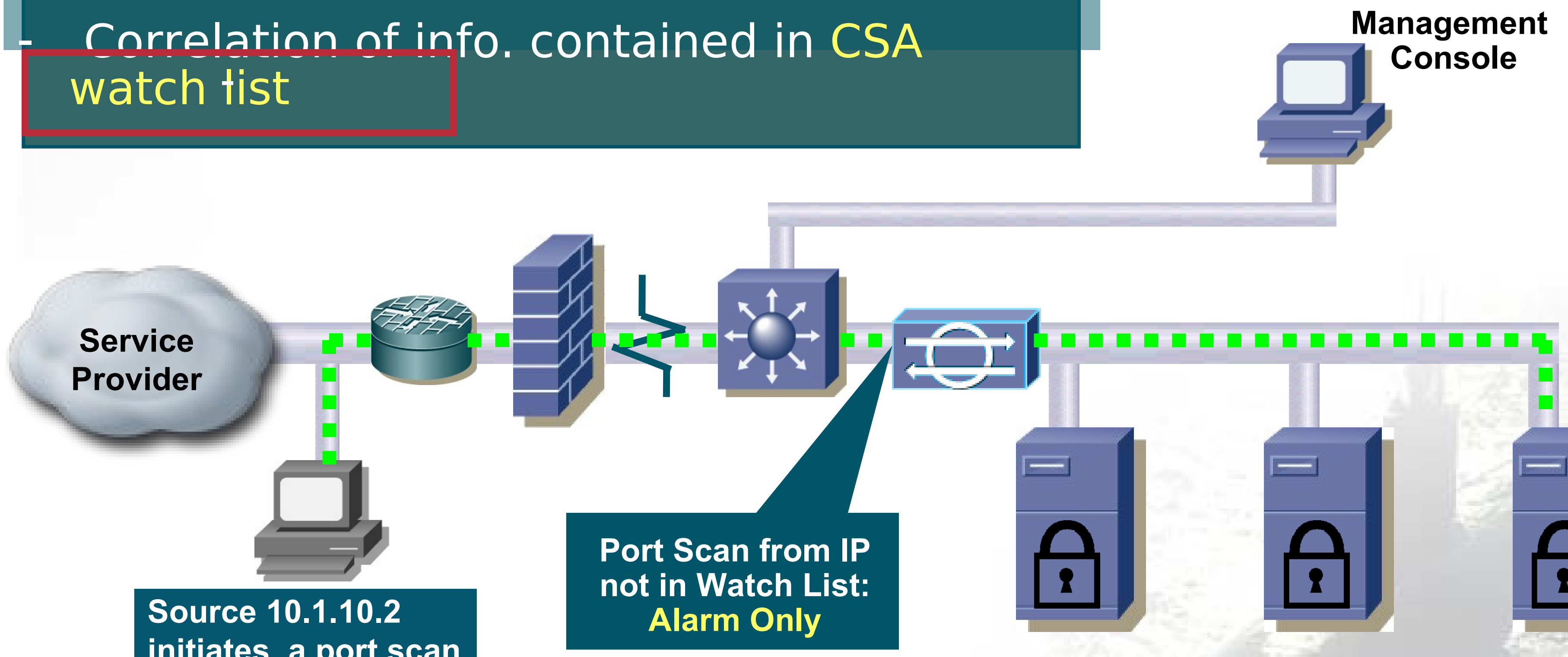
IDM is initialized successfully.

www.alefnula.com

IPS Version 6.0

IPS-CSA Collaboration

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list



Port Scan from IP not in Watch List: **Alarm Only**

Source 10.1.10.2 initiates a port scan destined for internal servers

ALEF NULA

DŮVĚŘUJTE SILNÝM

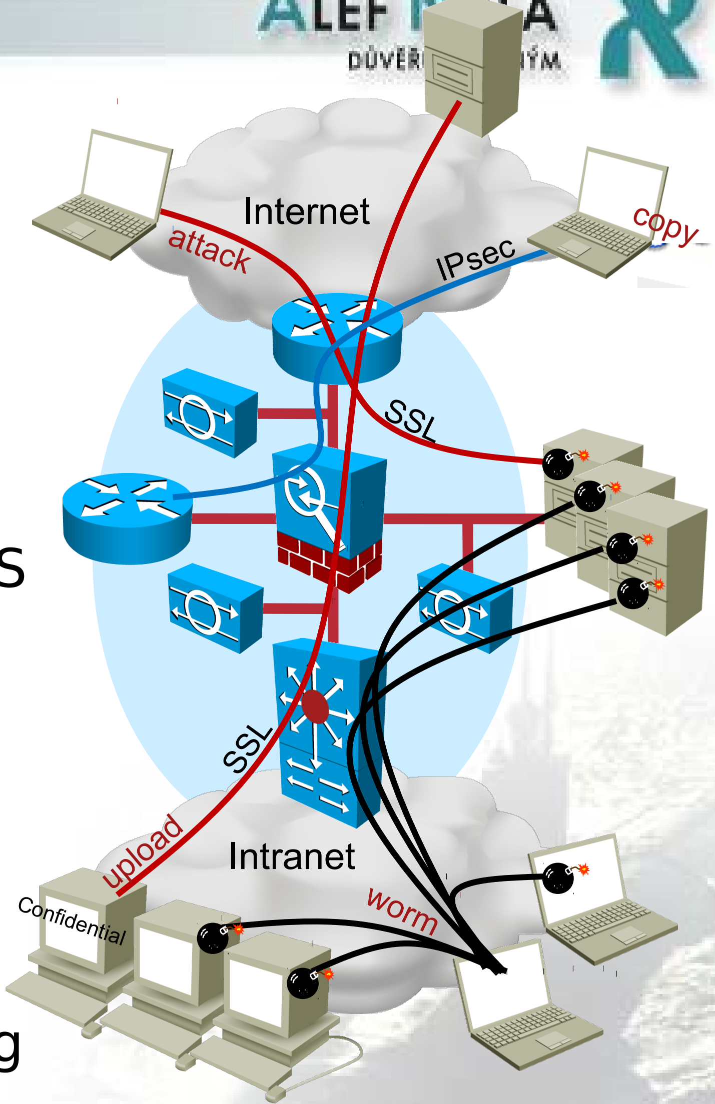
ENDPOINT SECURITY

Advanced Endpoint Security

Drivers

Challenges facing common security practices:

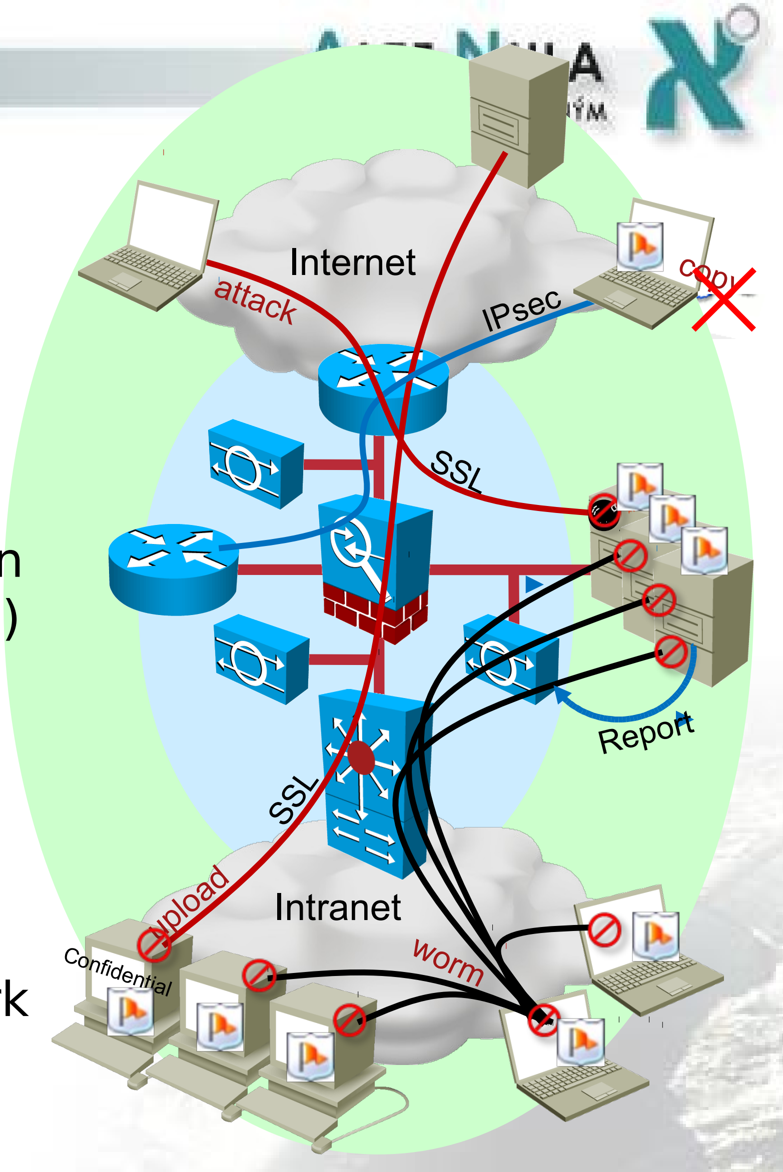
- New attacks that trick users into downloading malware cannot be stopped by signature-based mechanisms (e.g. IPS, AV)
- Encrypted end-to-end sessions (e.g. SSL) render firewalls and network IPS blind
- Network-based security devices cannot adequately control access to sensitive data (e.g. USB flash/disk, CD/DVD ROM, encrypted sessions)
- Security policies or regulatory requirements may be too demanding for the capabilities of network security solutions (e.g. PCI



Advanced Endpoint Security

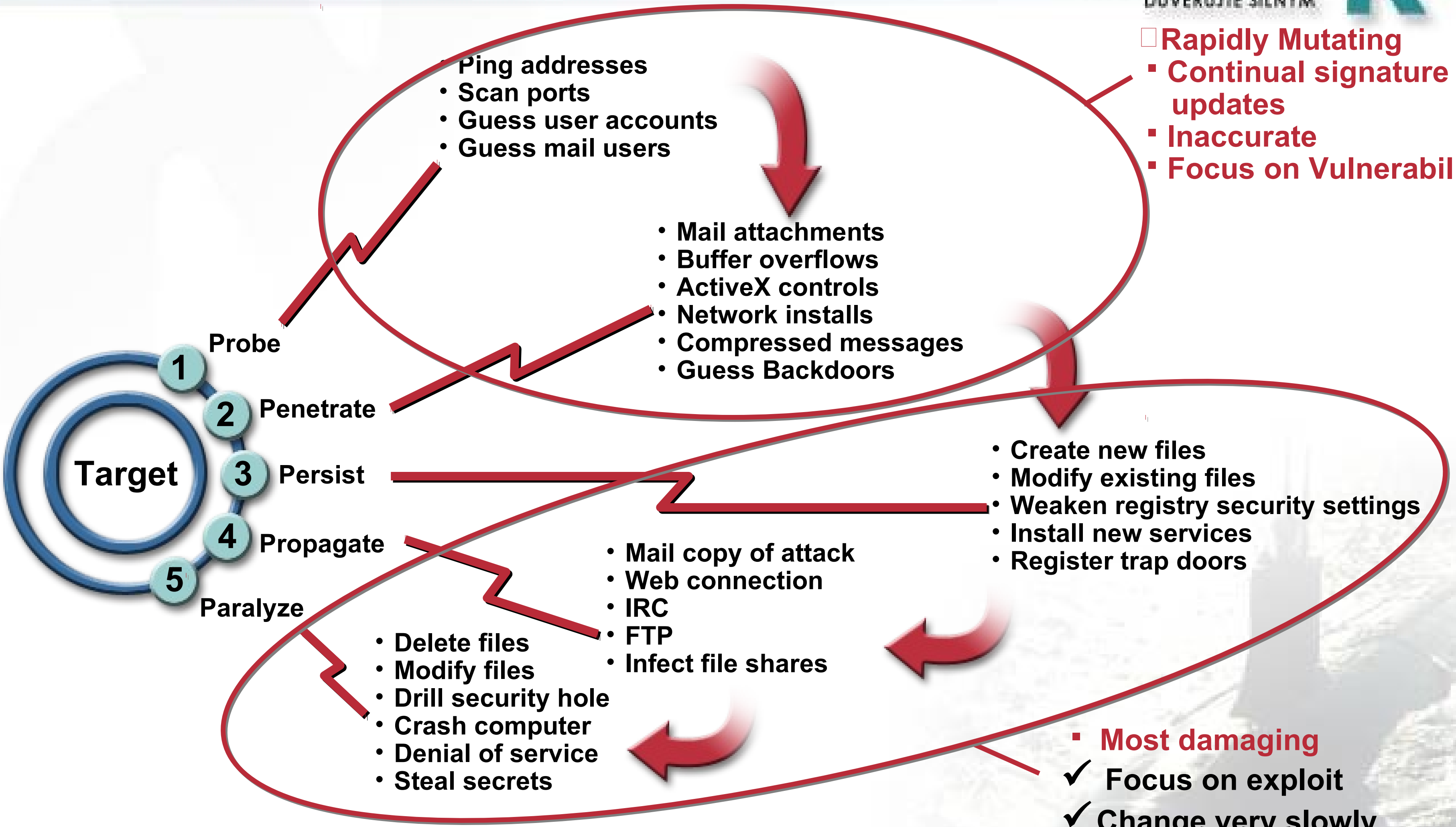
with Cisco Security Agent

- CSA extends network security solutions to end hosts
- Cisco Security Agent enhances security with:
- – **Zero Update protection** based on OS and application behavior
- – **Control of content** after decryption or before encryption (e.g. SSL, IPsec)
- – **Access control for I/O devices** based on process, network location and even file content
- – **Centralized management** and monitoring of events
- – **SDN Interaction** with other network solutions such as NAC, IPS, QoS, MARS, VOIP, etc



Copyright ALEF NULA, a.s. www.alefnula.com

CSA Approach:
Behavioral Protection for Endpoints



- Ping addresses
- Scan ports
- Guess user accounts
- Guess mail users

- Mail attachments
- Buffer overflows
- ActiveX controls
- Network installs
- Compressed messages
- Guess Backdoors

- Create new files
- Modify existing files
- Weaken registry security settings
- Install new services
- Register trap doors

- Mail copy of attack
- Web connection
- IRC
- FTP
- Infect file shares

- Delete files
- Modify files
- Drill security hole
- Crash computer
- Denial of service
- Steal secrets

□Rapidly Mutating

- Continual signature updates
- Inaccurate
- Focus on Vulnerability

- Most damaging

✓ Focus on exploit

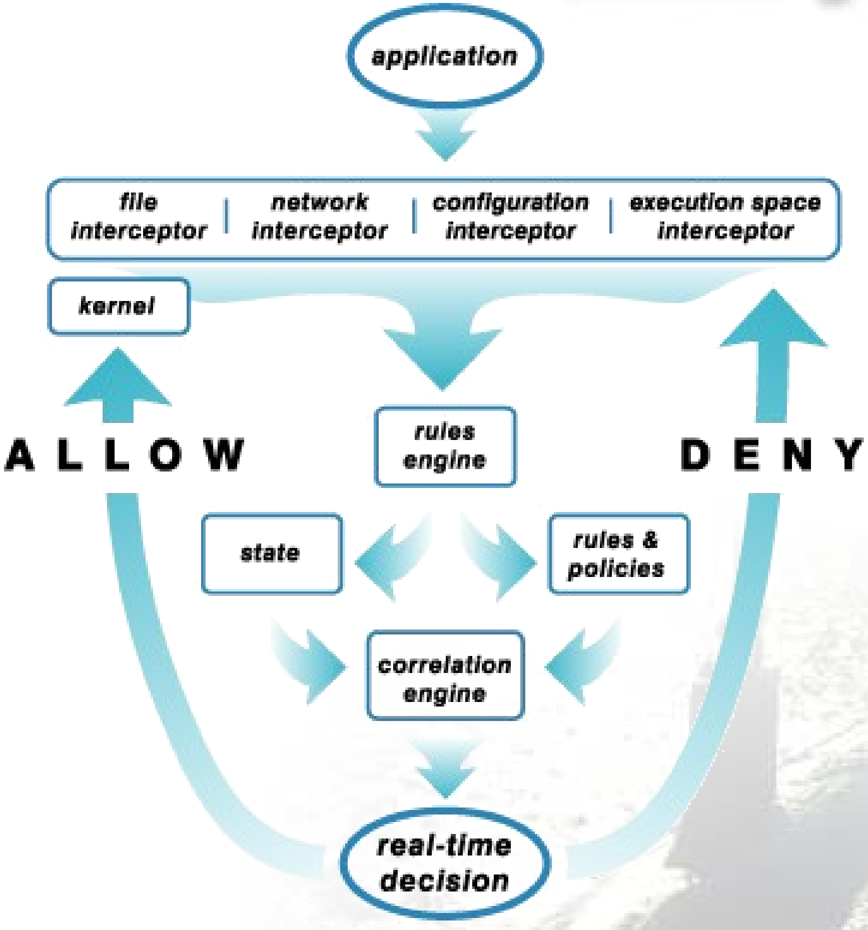
✓ Change very slowly

✓ Inspiration for Cisco Security Agent solution

CSA provides Network Collaboration

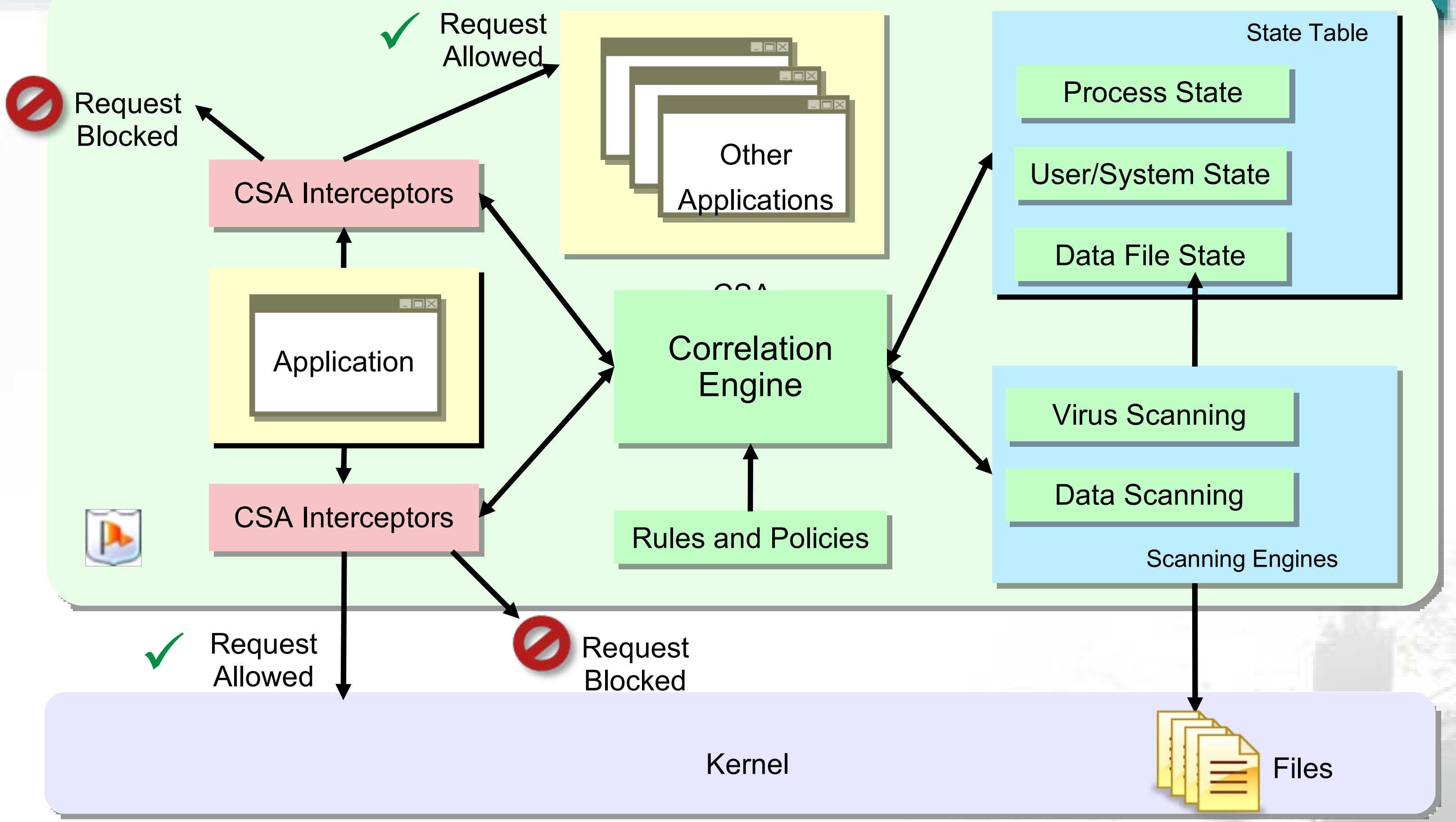
INCORE™ Architecture

- The Cisco Security Agent intercepts application OS calls and invokes an allow/deny response through a technology called INCORE:
- **INCORE**
  INtercept
  COrrelate
  Rules
  Engine
- “Zero Update” architecture – you don’t need a new signature to stop the next attack



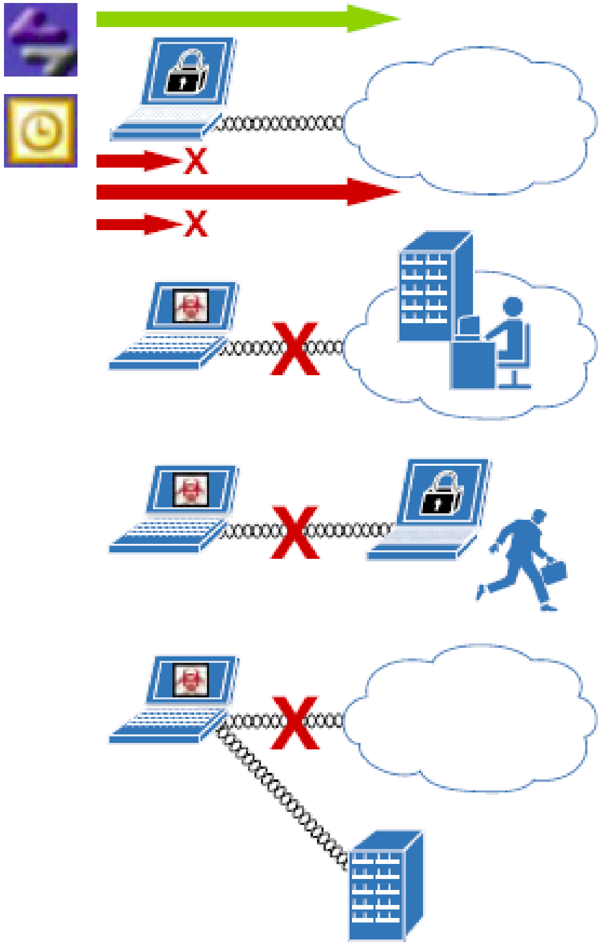
How CSA works

Intercepting and Correlating Operating System Calls



- CSA intercepts calls to the operating system, and also it verifies application calls for system resources against the policy
- “Zero Update” Architecture- policy based control, you don’t a new signature to stop an attack

Wireless Controls



Per-application Qos Prioritization

Disable wireless NIC when wired is active

Connection restrictions – certain SSIDs, Encryption, Ad-Hoc

Require VPN connection when out of the office

Data Loss Prevention

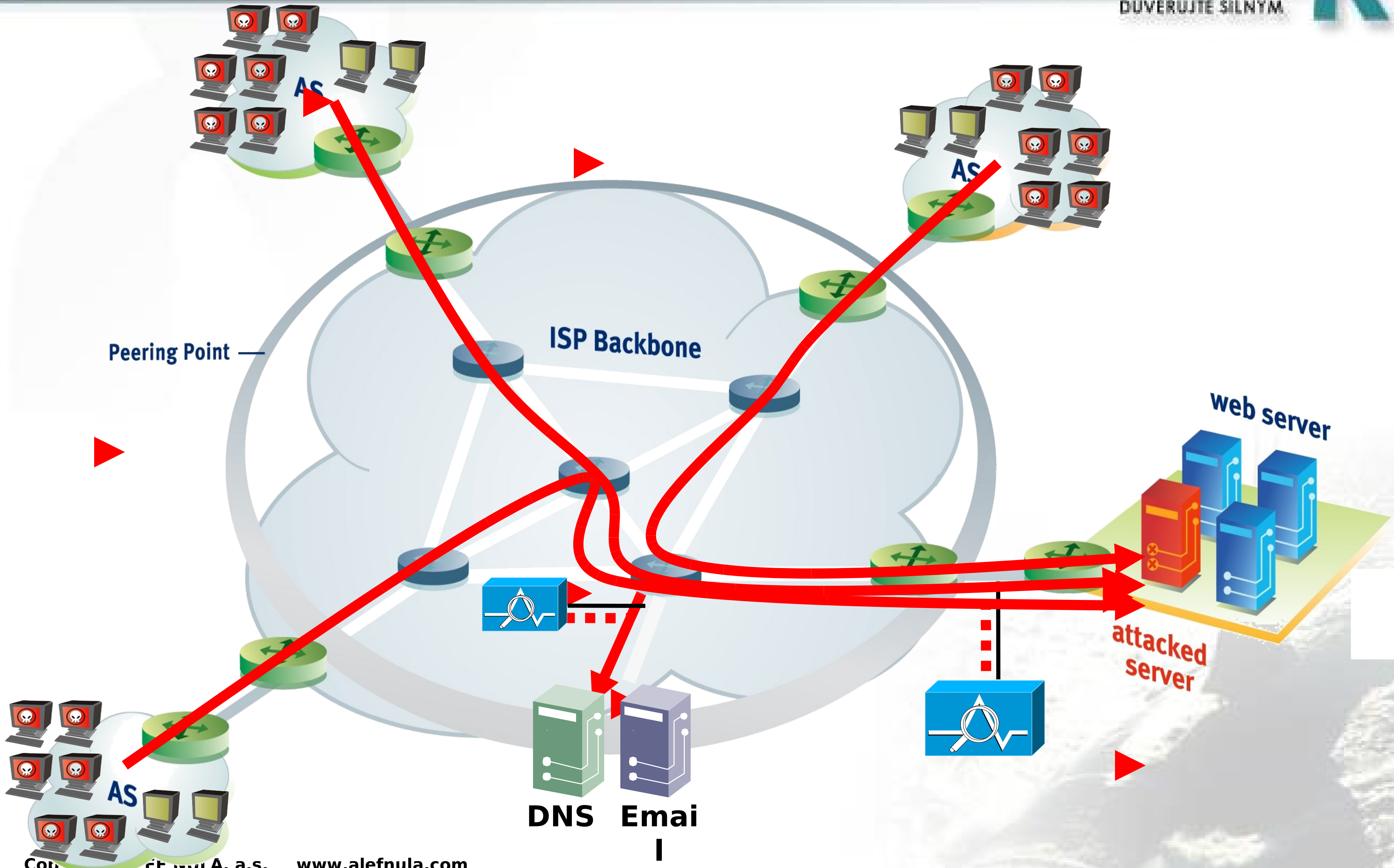
Data Theft Prevention Feature	CSA Capability
Control over removable media	– Dynamic tracking of applications that handle sensitive information – Prevents writing of sensitive information to removable media – USB, CD-ROM, floppy, etc.
Control over the Windows Clipboard	– Dynamic tracking of applications that copy and paste data – Prevents clipboard access to untrusted applications
Control over network transfers	– Dynamic tracking of applications that handle sensitive information – Prevents any network access for these applications

ALEF NULA

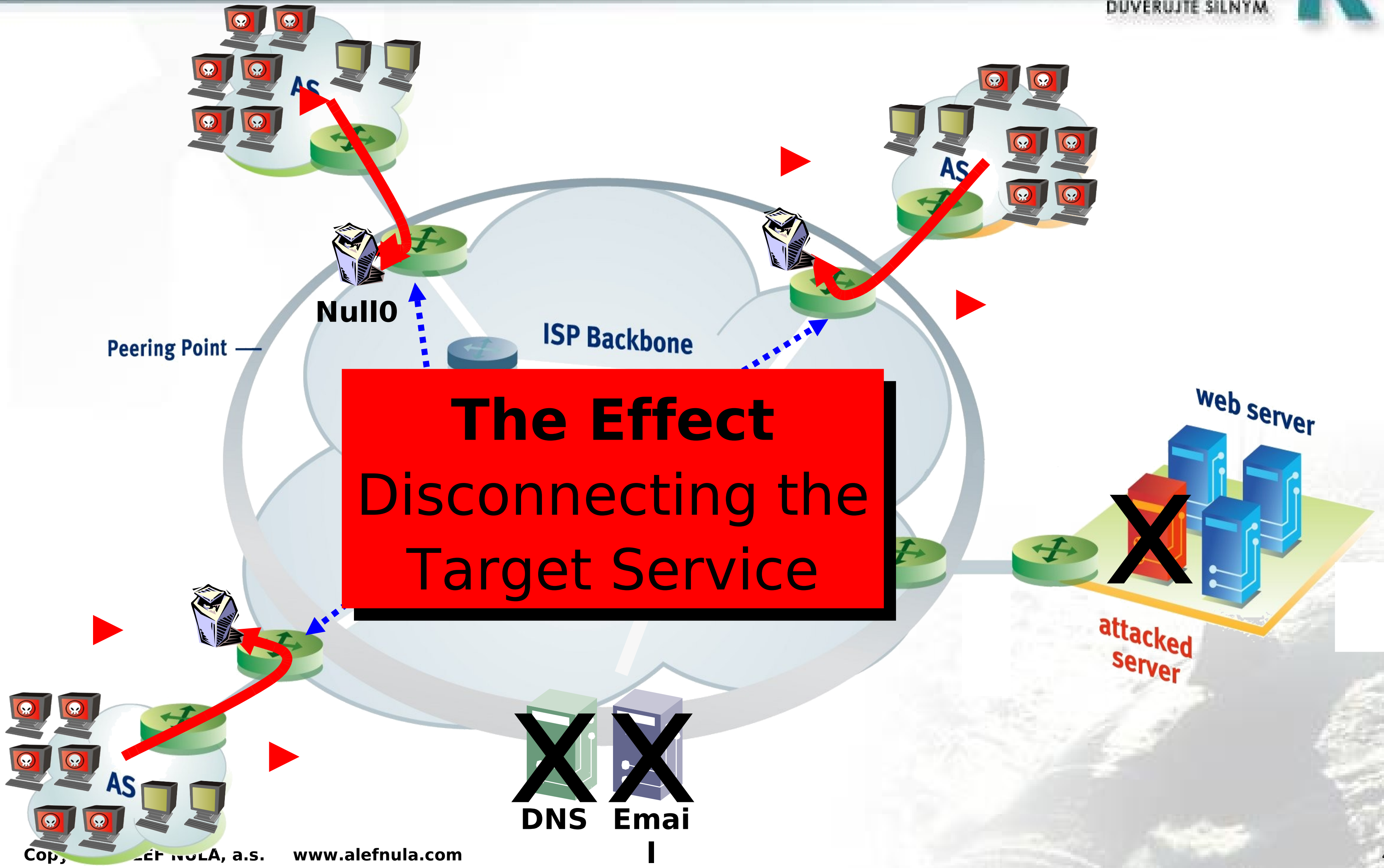
DŮVĚŘUJTE SILNÝM

DDoS MITIGATION SOLUTION

DDoS Attack Scenario



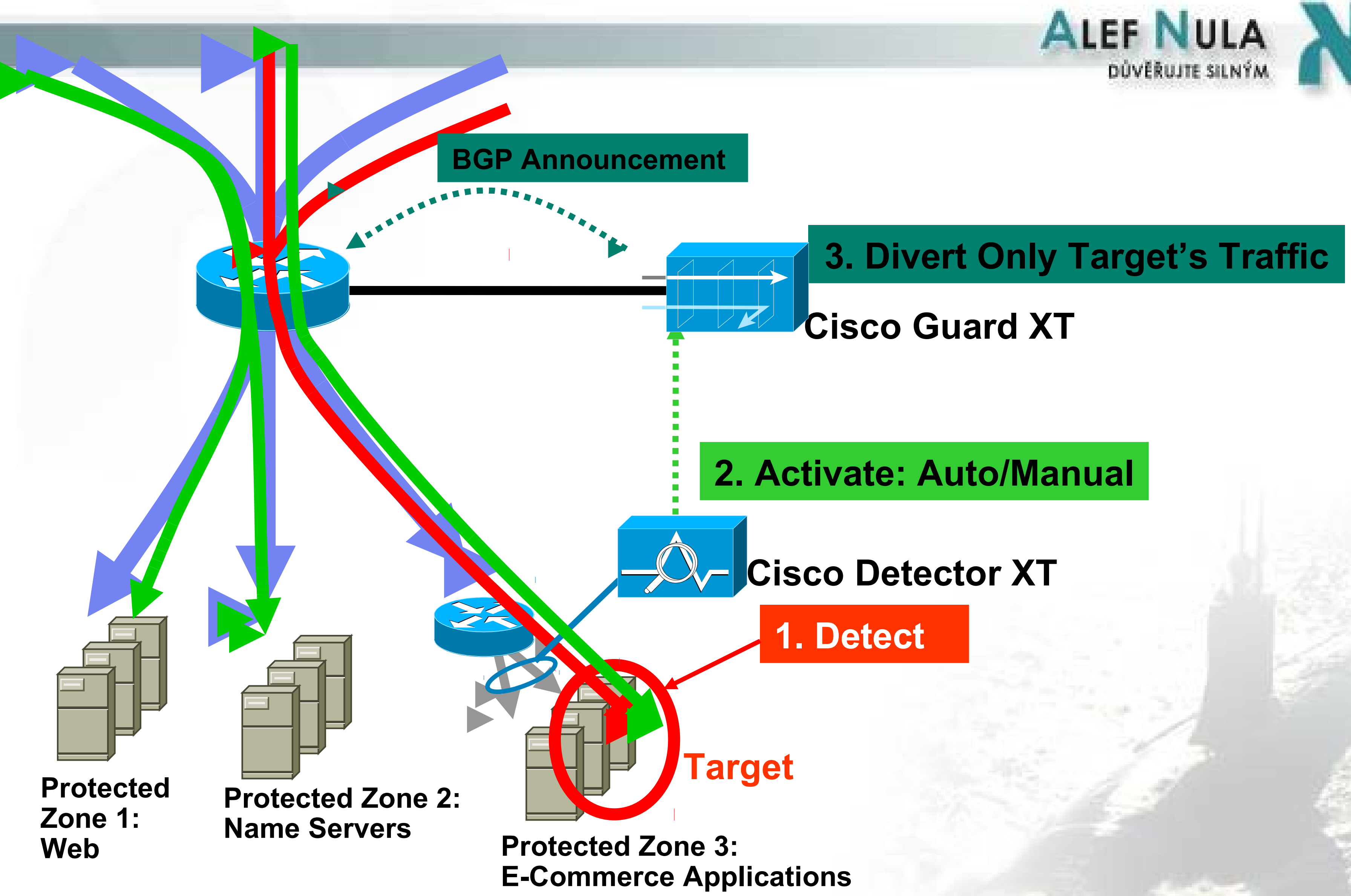
Today’s Black-hole technique



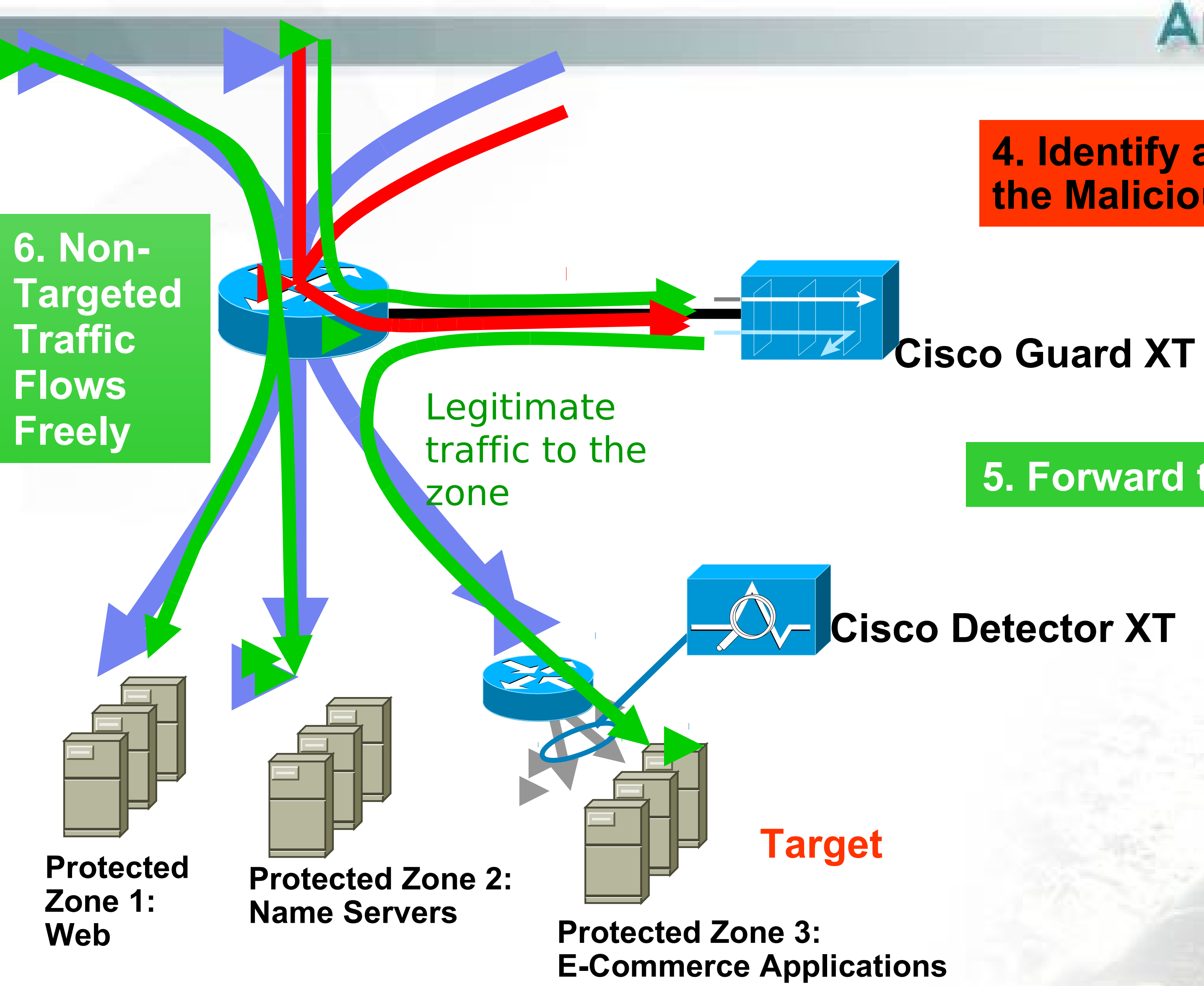
The Effect

Disconnecting the Target Service

DDoS Solution Operation

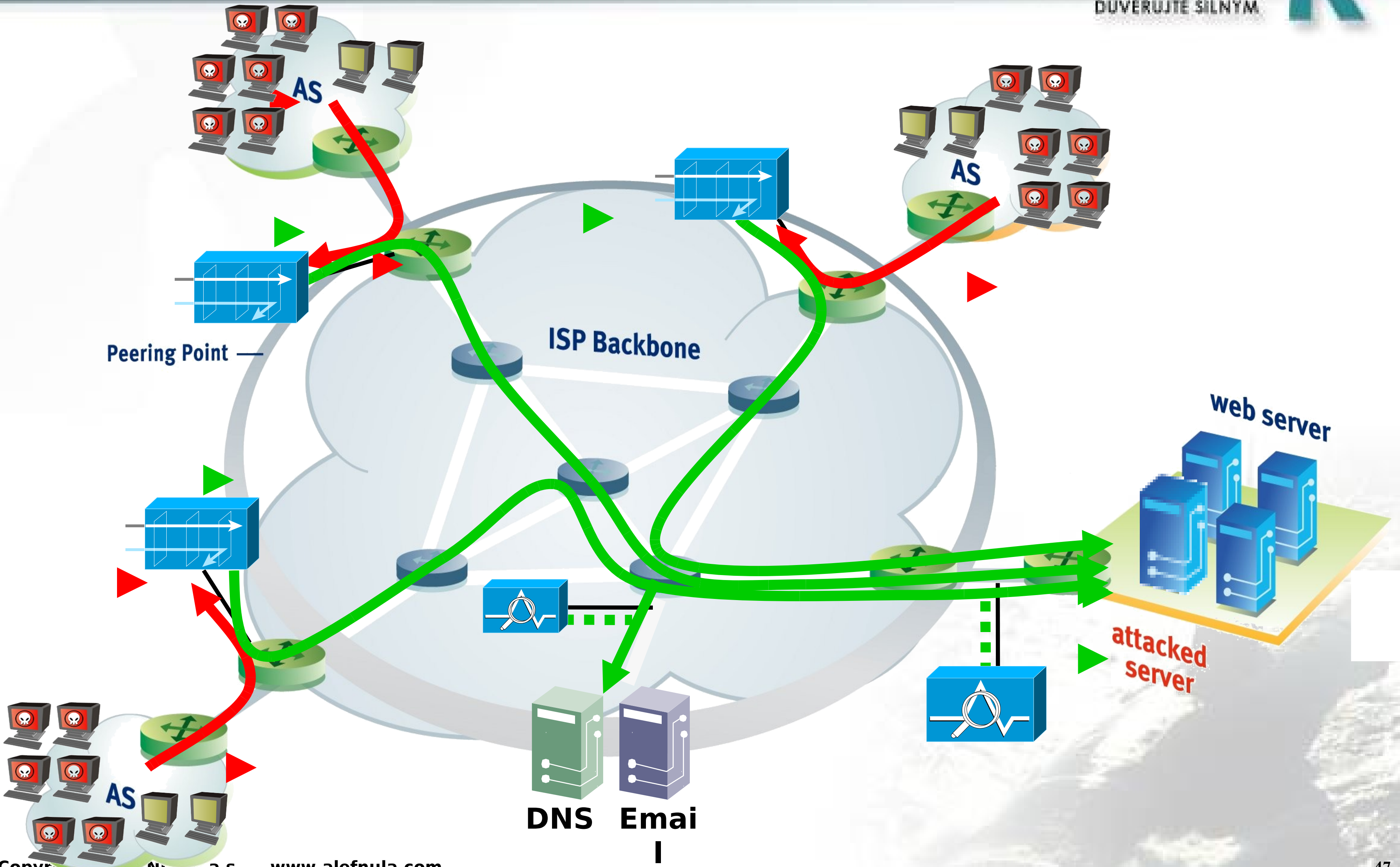


DDoS Solution Operation



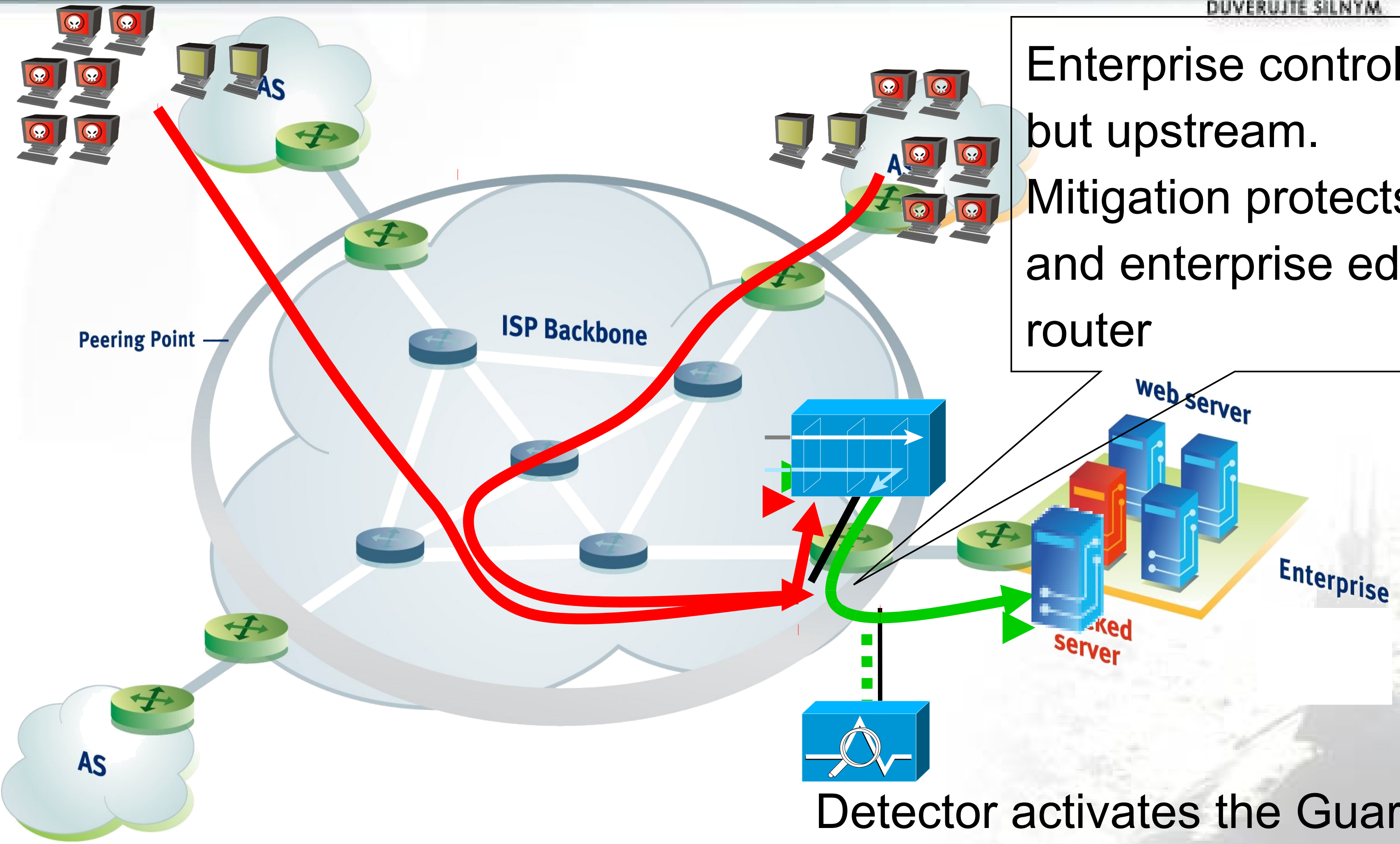
4. Identify and Filter the Malicious
6. Non-Targeted Traffic Flows Freely
Cisco Guard XT
Legitimate traffic to the zone
5. Forward the Legitimate
Cisco Detector XT
Target
Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Applications

Diversion at Peering Points



Enterprise Protection Upstream

Guard Co-Located at Provider Edge



Enterprise controlled, but upstream.
Mitigation protects link and enterprise edge router

Detector activates the Guard via separate management circuit

Multistage Verification Process™ (MVP)

Static Packet Filters

filter out packets according to pre-defined rules

Dynamic Packet Filters

filter out packets Per Flow, Protocol, Source IP

Anti-Spoofing Mechanisms

filter out packets from spoofed sources

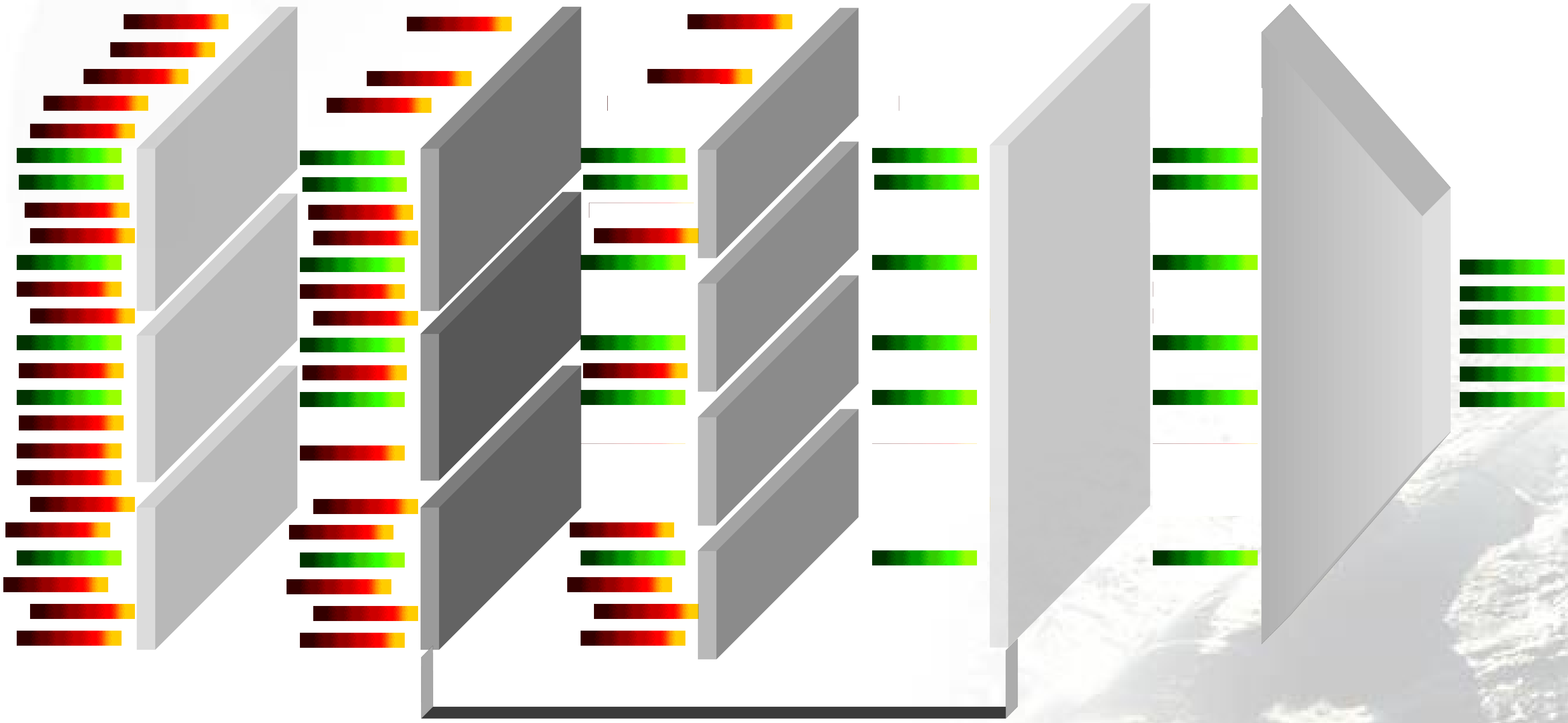
Statistical Inspection

Anomaly Recognition

per flow compared to a baseline

Rate-limiting

of traffic towards the zone



Adding Dynamic-Filters

Rate-