



*TOMORROW
starts here.*

Cisco *live!*



Web Security Deployment with WSA

BRKSEC-3771

Choo-Kai Kang (CK), Consulting Systems Engineer

#clmel

Cisco *live!*

Agenda

- Introduction and Housekeeping
- Deploying WSA in IPv4 & IPv6 Networks
 - Explicit Deployment
 - Transparent Deployment with WCCP
 - Deployment with Load balancer
 - Deployment with CARP (New)
 - Deployment with Advanced Malware Protection
- Deploying with Authentication
 - Transparent User Identification using CDA
 - Kerberos Authentication
- Troubleshooting Performance Issues



Housekeeping

- Hold questions and comments – plenty of Question Time at the end
- Keep your gadgets in silent mode
- Take any calls outside
- Do unto others...
- Will re-post slides and distribute via email

For Your Reference

- There are (many...) slides in your print-outs that will not be presented.
- They are there “For your Reference”



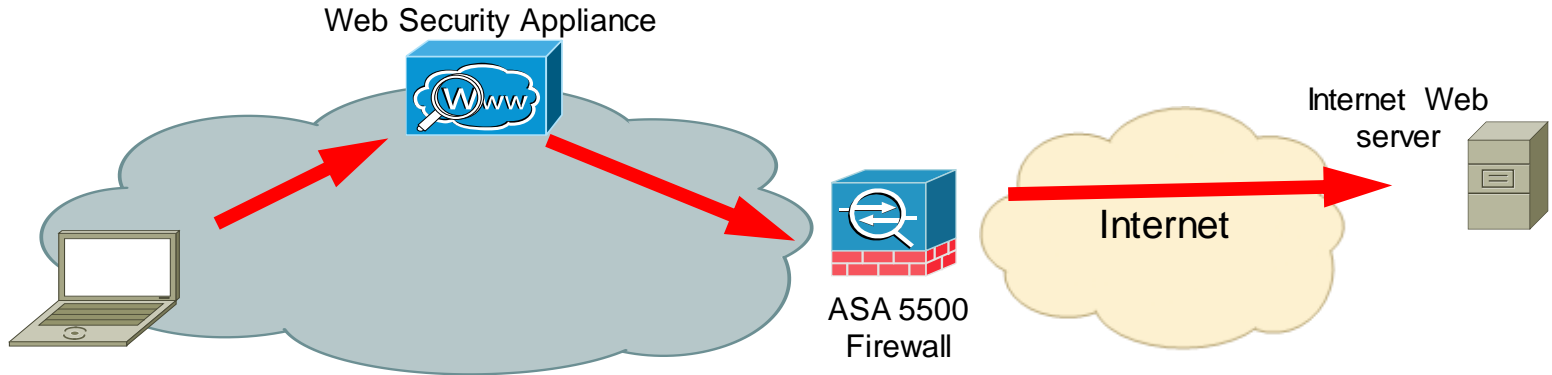
For Your
Reference



Explicit Deployment

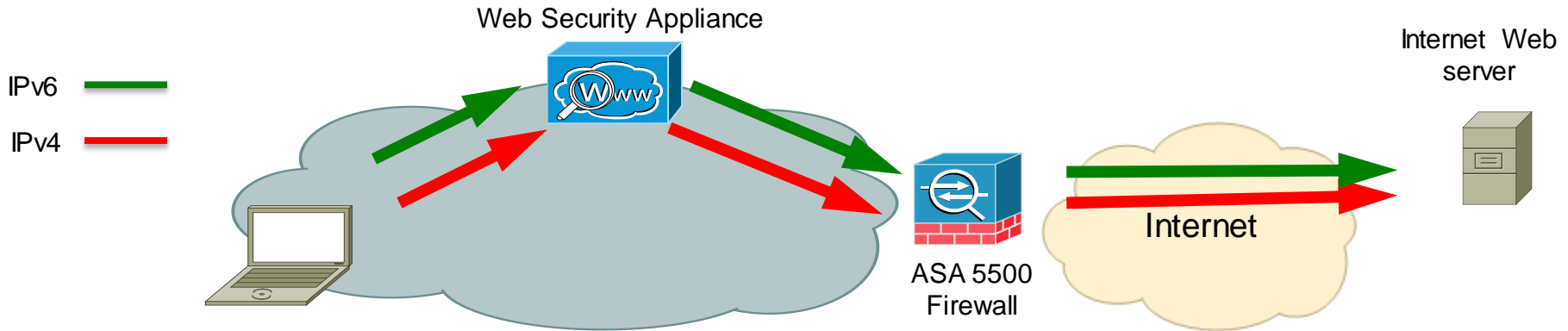
Explicit Proxy

- Client requests a website
- Browser connects first to WSA
- WSA connects to website
- Firewall usually only allows webtraffic for WSA
- DNS Resolution is done by WSA



Explicit Proxy with IPv4 & IPv6

- Client requests a website
- Browser connects first to WSA using IPv4 or IPv6
- WSA does DNS lookup
 - A record returned and/or AAAA record returned
- Depending on WSA setting, WSA builds outgoing connection either on IPv4 or IPv6



Explicit Mode with IPv4 & IPv6

- Setting IPv6 Addresses on the Interfaces

Interfaces			
Interfaces:	Ethernet Port	IP Address / Netmask	Hostname
	M1	IPv4: 172.16.2.66/24	wsa-ipv6.falcon.lab
		IPv6: 2001: [REDACTED] :6466/64	
	P1	IPv4: 192 [REDACTED] 3/28	wsa-ipv6p1.falcon.lab
		IPv6: 2001: [REDACTED] :3/64	
Separate Routing for Management Services:	No separate routing (M1 port used for both data and management)		
Appliance Management Services:	FTP on port 21, SSH on port 22, HTTP on port 8080, HTTPS on port 8443, Redirect HTTP request to HTTPS		
L4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)		
Edit Settings...			

Explicit Mode with IPv4 & IPv6

- Setting IPv6 Routes

IPv6 Routes for Management and Data Traffic (Interface M1: 2001:67c:2274:4041::6466, Interface P1: 2001:67c:2274:4012::3)

Add Route... Save Route Table... Load Route Table...

Route Name	Destination	Gateway	All <input type="checkbox"/> Delete
Clientnetzv6	2001: [REDACTED] :/64	2001: [REDACTED] :254	<input type="checkbox"/>
VPNPool	fd00:1:2:3::/64	2001: [REDACTED] :254	<input type="checkbox"/>
Default Route	All Other	2001: [REDACTED] :1	

Delete

Explicit Mode with IPv4 & IPv6

- Setting DNS Servers

DNS Server Settings

DNS Servers: Use these DNS Servers

Priority ?	Server IP Address	
<input type="text" value="0"/>	<input type="text" value="2001:db8:1:10::201"/>	<input type="button" value="Add Row"/> <input type="button" value="Delete"/>

Alternate DNS servers Overrides (Optional):

Domain(s)	DNS Server IP Address(es)
<input type="text"/>	<input type="text"/>

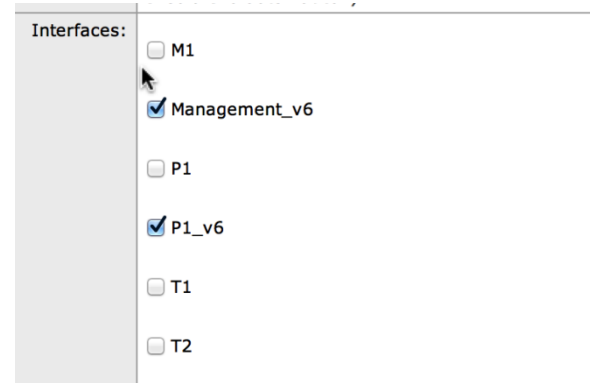
i.e., example.com, example2.com *i.e., 10.0.0.3 or 2001:420:...*

Which Protocol should be preferred in case of A and AAAA record returned?

Routing Table for DNS Traffic:	Management
IP Address Version Preference:	<input type="radio"/> Prefer IPv4 <input checked="" type="radio"/> Prefer IPv6 <input type="radio"/> Use IPv4 only <i>This preference applies when DNS results provide both IPv4 and IPv6 address for host.</i>
Timing out Reverse DNS Lookups:	<input type="text" value="20"/> seconds

Packet Capture with IPv6

- Packet Capture shows additional interfaces for IPv4 & IPv6
- Filter can be applied to IPv6 addresses



Packet Capture Settings	
Capture File Size Limit:	200 MB
Capture Duration:	Run Capture Indefinitely
Interfaces Selected:	Management_v6, P1_v6
Filters Selected:	(tcp port 80 or tcp port 3128) and host fd00:1:2:3::1

[Edit Settings...](#)

CLI

- Neighbour Cache in IPv6 is equivalent to the arp cache in IPv4

AsyncOS 8.0.0 for Web build 387

Welcome to the Cisco S100V Web Security Virtual Appliance

```
munlab-vwsa1.munsec.com> arp
```

Display the arp-cache

```
munlab-adc.munsec.com (172.16.10.30) at 00:0c:29:2d:b3:80 on em0 expires in 1178 seconds [ethernet]
munlab-spyker1.munsec.com (172.16.10.220) at 44:d3:ca:34:ea:1f on em0 expires in 492 seconds [ethernet]
munlab-cda.munsec.com (172.16.10.29) at 00:0c:29:6d:ad:83 on em0 expires in 1158 seconds [ethernet]
munlab-c6504.munsec.com (172.16.10.66) at 00:07:7d:75:05:c0 on em0 expires in 188 seconds [ethernet]
munlab-3560.munsec.com (172.16.10.10) at 44:d3:ca:2f:f0:c1 on em0 expires in 360 seconds [ethernet]
munlab-vwsa1.munsec.com> ndp
```

```
Neighbor                               Linklayer Address  Netif Expire   S Flags
fe80::20c:29ff:feee:b5ab%gre0         (incomplete)      gre0 permanent R
fe80::20c:29ff:feee:b5d3%em4          0:c:29:ee:b5:d3   em4 permanent R
fe80::20c:29ff:feee:b5c9%em3          0:c:29:ee:b5:c9   em3 permanent R
fe80::20c:29ff:feee:b5bf%em2          0:c:29:ee:b5:bf   em2 permanent R
fe80::20c:29ff:feee:b5b5%em1          0:c:29:ee:b5:b5   em1 permanent R
fe80::46d3:caff:fe2f:f0c1%em0         44:d3:ca:2f:f0:c1 em0 23h59m48s S R
munlab-vwsa1.munsec.com                0:c:29:ee:b5:ab   em0 permanent R
2001:420:44e6:2013::66                 0:7:7d:75:5:c0   em0 26s          R R
fe80::4603:a7ff:fe32:c541%em0         44:3:a7:32:c5:41 em0 23h41m32s S R
fe80::207:7dff:fe75:5c0%em0           0:7:7d:75:5:c0   em0 3s           D R
fe80::20c:29ff:feee:b5ab%em0          0:c:29:ee:b5:ab   em0 permanent R
2001:420:44e6:2013::10                 44:d3:ca:2f:f0:c1 em0 12s          R R
munlab-adc.munsec.com                  0:c:29:2d:b3:80   em0 28s          R
munlab-vwsa1.munsec.com
```

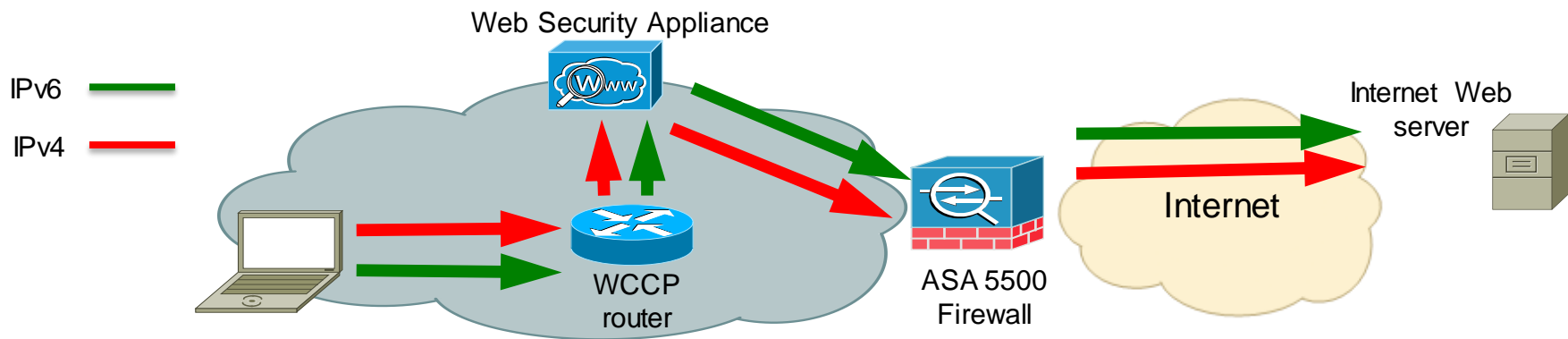
Display the neighbour table



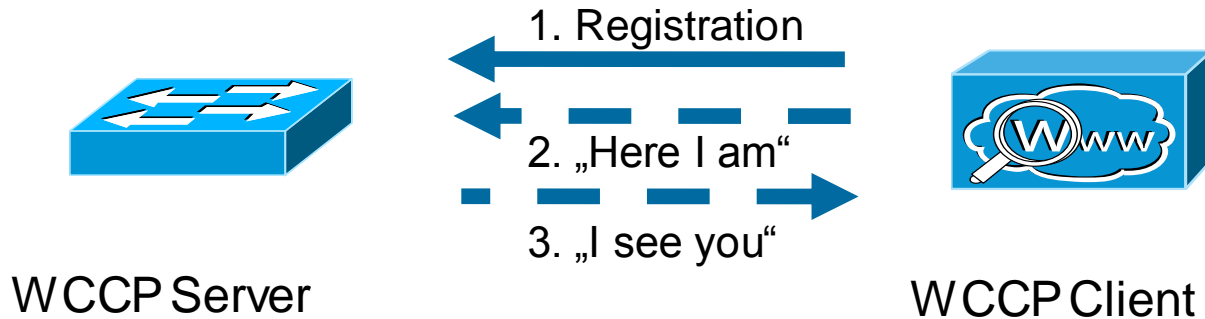
Deploying WCCP

Transparent Proxy via WCCP

- Client requests a website
- Browser tries to connect to Website
- Network Device redirects traffic to WSA using WCCP
- WSA proxies the request
- DNS Resolution is done by the Client



How WCCP Registration Works



- The WCCP client registers at the WCCP Server
- Both, Server and Client need to use the same WCCP Service Group ID
- One WCCP Server usually can server multiple Clients
- Server and Client exchange „here i am“ and „I see you“ Packets to check availability
 - UDP/2048, unicast
 - Multicast possible
- Traffic is redirected from Server to one or multiple Clients using the „hash“ or „mask“ algorithm

WCCP Protocol - Buckets

Hash Based Assignment

Byte level (8 bit) XOR computation divided into 256 buckets (default)

Mask Based Assignment

Bit level AND divided up to 128 buckets (7 bits)

```
munlab-spyker1/actNoFailover# show wccp 90 buck
```

```
WCCP hash bucket assignments:
```

```
Index  Cache Engine:
00     172.16.40.100
01     172.16.10.45
FF     NOT ASSIGNED
```

```
XX| 0 1 2 3 4 5 6 7 8 9 A B C D E F
--|-----
00| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
10| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
20| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
30| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
40| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
50| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
60| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
70| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
80| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
90| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
A0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
B0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
C0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
D0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
E0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
F0| 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
```

```
asa# show wccp 90 hash 144.254.1.1
172.16.10.71 80 1024
```

WCCP hash information for:

Primary Hash: Dst IP: 144.254.1.1

Bucket: 110

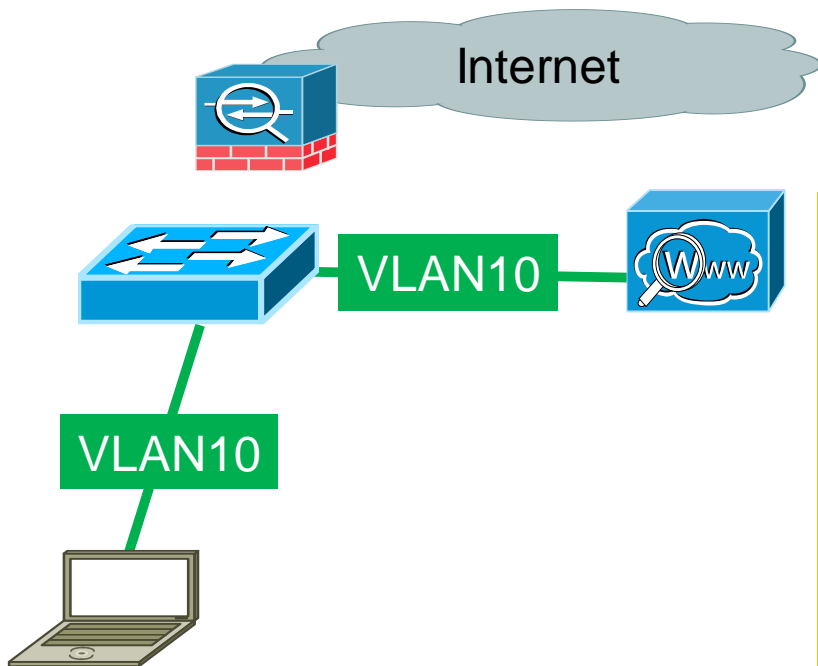
Cache Engine: 172.16.10.45

Using WCCP for Traffic Redirection (2)

- Performance Considerations:
- MASK (HW) > HASH (SW)
 - HW has to take TCAM Resources into consideration
- L2 (HW) > GRE (SW)
- Use GRE if WSA is located in other subnet
 - Check if Device can do GRE in HW
- User L2 if WSA and WCCP Device are in same subnet

WCCP with L3 Switch (3560/3750)

L2 Redirect

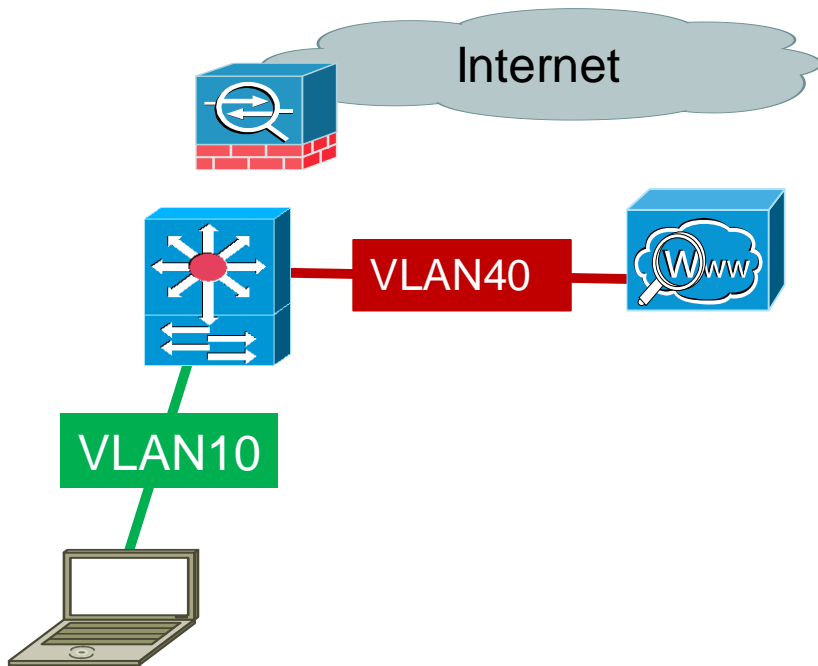


Use template “access”, “routing” or “dual-ipv4/ipv6 routing”
WCCP shares same TCAM Region than PBR!

```
sdm prefer routing
ip routing
ip wccp 91 redirect-list wsa
ip access-list extended wsa
  permit tcp any any eq www
  permit tcp any any eq 443
!
interface Vlan10
  ip address 172.16.10.10
  255.255.255.0
  ip wccp 91 redirect in
```

WCCP IPv6 & IPv4

Different service groups for IPv4 & IPv6



```
ip wccp 90 redirect-list wsav4
ipv6 wccp 91 redirect-list wsav6
!
interface Vlan10
 ip address 172.16.10.10 255.255.255.0
 ipv6 address 2001:db8:1:10::66/64
 ipv6 nd ra suppress
 ip wccp 90 redirect in
 ipv6 wccp 91 redirect in

ipv6 access-list wsav6
 permit tcp 2001:DB8:1:10::/64 any eq www
 permit tcp 2001:DB8:1:10::/64 any eq 443
!
ip access-list extended wsav4
 permit tcp any any eq 80
 permit tcp any any eq 443
```

WCCP with L3 Switch

Redirect - Verification

```
munlab-3560X#show ip wccp 91 detail
```

```
WCCP Client information:
```

```
WCCP Client ID:      172.16.10.100
```

```
Protocol Version:    2.0
```

```
State:               Usable
```

```
Redirection:         L2
```

```
Packet Return:       L2
```

```
Packets Redirected:  0
```

```
Connect Time:        01:02:16
```

```
Assignment:          MASK
```

```
Mask  SrcAddr  DstAddr  SrcPort  DstPort
```

```
----  -
```

```
0000: 0x00000000 0x00000526 0x0000  0x0000
```

```
Value SrcAddr  DstAddr  SrcPort  DstPort  CE-IP
```

```
-----
```

```
0000: 0x00000000 0x00000000 0x0000  0x0000  0xAC100A64 (172.16.10.100)
```

```
0001: 0x00000000 0x00000002 0x0000  0x0000  0xAC100A64 (172.16.10.100)
```

```
0002: 0x00000000 0x00000004 0x0000  0x0000  0xAC100A64 (172.16.10.100)
```

Version & State

Redirect Method

Assignment Method

Mask Value

WCCP with L3 Switch – IPV6

Redirect - Verification

```
munlab-c6504#sh ipv6 wccp 90 det
```

```
WCCP Client information:
```

```
WCCP Client ID:      2001:420:44E6:2013::45
```

```
Protocol Version:    2.01
```

```
State:               Usable
```

```
Redirection:         L2
```

```
Packet Return:       L2
```

```
Assignment:          MASK
```

```
Connect Time:        00:13:25
```

```
Redirected Packets:
```

```
  Process:           0
```

```
  CEF:               0
```

```
GRE Bypassed Packets:
```

```
  Process:           0
```

```
  CEF:               0
```

```
Mask Allotment:      4 of 4 (100.00%)
```

```
Assigned masks/values: 1/4
```

```
Mask  SrcAddr  DstAddr  SrcPort  DstPort
```

```
-----  
0000:  ::      300::    0x0000  0x0000
```

**Version &
State**

**Redirect
Method**

**Assignment
Method**

Mask Value

WCCP with L3 Switch (CAT6500)

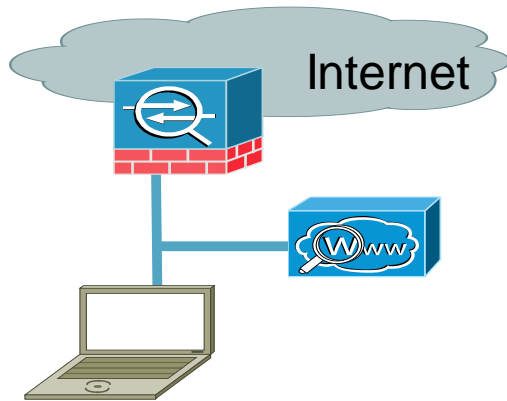
L2 or GRE Redirect

- Ingress - L2 redirection + Hash Assignment (Requires SW Processing)
- **Ingress - L2 redirection + Mask Assignment (Full HW Processing - recommended)**
- Egress - L2 redirection + Hash Assignment (Requires SW Proc.)
- Egress - L2 redirection + Mask Assignment (Requires SW Proc.)

First packet is process switched, creates netflow entry. Subsequent packets are HW switched

- Ingress - L3 (GRE) redirection + Hash Assignment (Requires SW Proc.)
- **Ingress - L3 (GRE) redirection + Mask Assignment (Full HW Processing - Sup32/Sup720/2T only)**
- Egress - L3 (GRE) redirection + Hash Assignment (Requires SW Proc.)
- Egress - L3 (GRE) redirection + Mask Assignment (Requires SW Proc.)

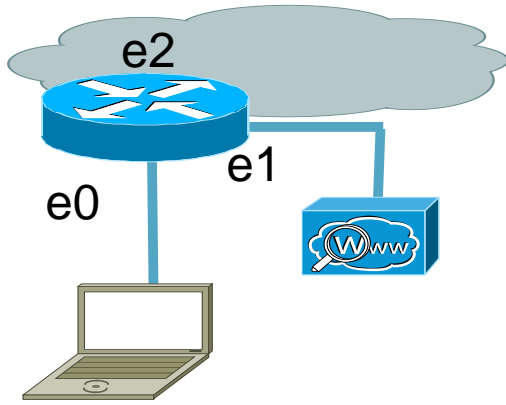
WCCP with ASA



- ASA allows only „redirect in“
 - Client and WSA must be on same interface
 - No DMZ Deployment possible...☹
- Inside ACL is checked before redirection
 - Destination Server must be allowed in ACL
- Redirection Method is GRE based
- Redirect ACL allows permit and deny

```
access-list WCCPRedirectionList extended deny ip 172.16.10.0
255.255.255.0 172.16.10.0 255.255.255.0
access-list WCCPRedirectionList extended permit tcp any any eq www
access-list WCCPRedirectionList extended permit tcp any any eq https
!
wccp 90 redirect-list WCCPRedirectionList
wccp interface INSIDE 90 redirect in
```


WCCP with Router – ISR, ISRG2



- Redirect is GRE and Hash
 - Done in SW
- Allows for DMZ-Design
- Supports „permit“ and „deny“ Statements in the redirection ACL

```
ip cef
ip wccp version 2
ip wccp 91 redirect-list <redirect-ACL>
!
interface e0
  ip wccp 91 redirect in
```

A Word About Hardware

- The “mask” Assignment is handled in Hardware on ASR, Cat6500,...
- WCCP redirect ACL deny statements don't use mask TCAM
- WCCP redirect ACL permit statements use up to the **Number of ACL Permit Entries * Number of Buckets**
- Example:
For a 7 bit mask, the router / switch is using 4096 TCAM entries for 32 permit statements...wasting lot of TCAM resources
- Adjusting the Bit-Mask must be done on the WCCP Client
 - Supported with v7.7 SW Release ☺

Advanced: Load-Balancing Method: Allow Mask Only

Mask: 0x 1526
Hex value between 0x1 and 0xFFFFFFFF

A Word About Hardware (2)

- 1-2 WSAs 1 bit, 2 slots
- 3-4 WSAs 2 bits, 4 slots
- 5-8 WSAs 3 bits, 8 slots
- 9-16 WSAs 4 bits, 16 slots
- 17-32 WSAs 5 bits, 32 slots

```
munlab-3560X#show ip wccp 90 detail
WCCP Client information:
  WCCP Client ID:      172.16.10.45
  Protocol Version:    2.0
  State:               Usable
  Redirection:         L2
  Packet Return:       L2
  Packets Redirected:  0
  Connect Time:        00:08:10
  Assignment:          MASK

  Mask  SrcAddr  DstAddr  SrcPort  DstPort
  ----  -
  0000: 0x00000000 0x00000003 0x0000  0x0000

  value SrcAddr  DstAddr  SrcPort  DstPort  CE-IP
  ----  -
  0000: 0x00000000 0x00000000 0x0000  0x0000  0xAC100A2D (172.16.10.45)
  0001: 0x00000000 0x00000001 0x0000  0x0000  0xAC100A2D (172.16.10.45)
  0002: 0x00000000 0x00000002 0x0000  0x0000  0xAC100A2D (172.16.10.45)
  0003: 0x00000000 0x00000003 0x0000  0x0000  0xAC100A2D (172.16.10.45)

munlab-3560X#
```

0x3 = 2 bits

4 slots for up to 4 WSA

Transparent Deployment - Summary

- No client settings necessary
- Client resolves hostname of target web server -> improved performance!
- Traffic gets redirected by the network
- Allows for redundancy by defining multiple WSAs to redirect
- Selection of the right WCCP device to redirect is critical.
- Try to limit down „Permit“ Entries in Redirect Lists for „Mask“ assignment, adjust mask in ASYNC-OS 7.7+

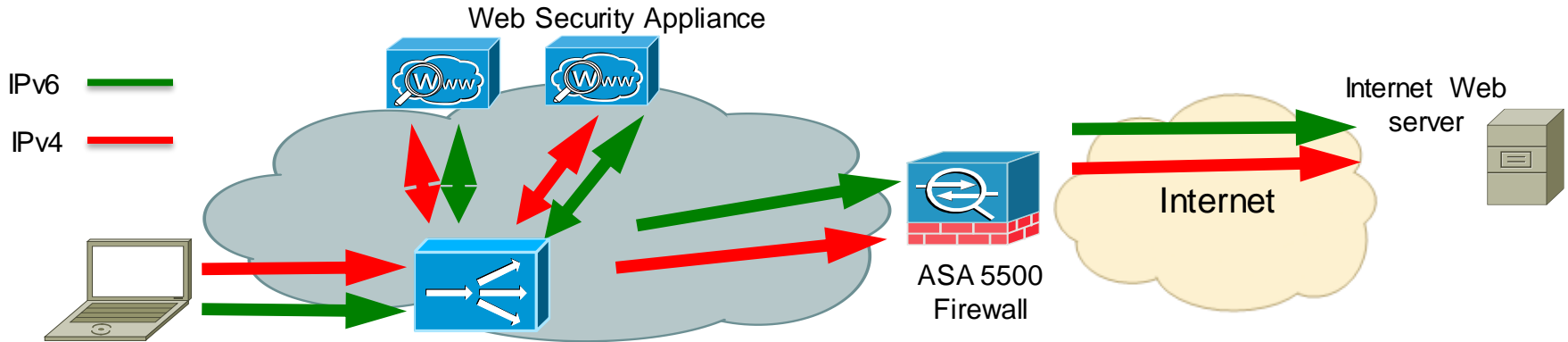
A nighttime photograph of a city street. In the background, there are modern buildings with lit windows and a pedestrian bridge with blue lighting. The foreground is dominated by long, curved light trails from cars, creating a sense of motion and energy. The overall scene is illuminated by city lights, with a mix of warm yellow and cool blue tones.

Deploying with Load Balancer

Loadbalancer Deployment

Using Netscaler VPX

- Client requests a website
- Loadbalancer redirects the traffic
- WSA proxies the request
- DNS Resolution depends on the client Setting (explicit or transparent with PBR)



Netscaler VPX – Server Definition

Configure Server [X]

Server Name:

IP Address Domain Name

IPAddress*: IPv6

Traffic Domain ID:

Translation IP Address:

Translation Mask:

Resolve Retry (secs):

Comments:

Resolve Domain Immediately

[?] [OK] [Close]

Can be IPv4 or IPv6

Define one Server per WSA System

Netscaler VPX – Service (1)

- Each Server requires a Service to define for what protocols this Server is used
- For WSA in this Example : HTTP

NetScaler > Traffic Management > Load Balancing > Services

Refresh | Help | Print

Add... Open... Remove Action Search

Name	State	IP Address/Domain Name	Traffic Domain ID	Port	Protocol	Max Clients	Max Requests	Cache Type
▶ WSA1	● Up	172.16.10.45	0	80	HTTP	0	0	SERVER
▶ WSA2	● Up	172.16.10.46	0	80	HTTP	0	0	SERVER

25 Per Page | 1 - 2 of 2 | 1

Each Server requires at least one
SERVICE.

Netscaler VPX – Service (2)

Configure Service

Service Name* WSA1

Protocol* HTTP

Traffic Domain 0

Service State UP

Enable Health Monitoring AppFlow Logging

Monitors

Policies

Profiles

Advanced

SSL Settings

Thresholds

Settings

Use Source IP Client Keep-Alive TCP Buffering

Client IP Header X-FORWARDED-FOR

Protocol that is used for this Service (HTTP)

X-FORWARDED-FOR Header is used to signal the Client IP to the WSA

Netscaler VPX – Virtual Server

- Define a virtual Server
- This the IP Address where a client will connect to when used in explicit mode

NetScaler > Traffic Management > Load Balancing > Virtual Servers

Refresh Help Print

Add... Open.. Remove Action Search ▾

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Method	Persistence	% Health
▶ WSProxy	Up	Up	172.16.10.52	0	80	HTTP	LEASTCONNECTION	SOURCEIP	100.00% 2 UP/0 DOWN

25 Per Page ▾ | 1 - 1 of 1 | 1 ▾

Netscaler VPX – Virtual Server (2)

Configure Virtual Server (Load Balancing)

Name* IP Address Based IP Pattern Based

Protocol* IP Address*

Network VServer Range Port*

State UP AppFlow Logging Traffic Domain ID

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

[Activate All](#) [Deactivate All](#)

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
<input checked="" type="checkbox"/>	WSA1	172.16.10.45	80	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0
<input checked="" type="checkbox"/>	WSA2	172.16.10.46	80	HTTP	<input checked="" type="radio"/> UP	<input type="text" value="1"/>	0

Comments

Services are mapped to the Virtual Server

Netscaler VPX – Virtual Server (3)

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

LB Method

Method **Least Connection** New Service Startup Request Rate PER_SECOND

Current Method: Round Robin
Reason: Bound service's state changed to UP

Persistence

Persistence **SOURCEIP**

Time-out (min)

IPv4 Netmask

IPv6 Mask Length

Comments

SOURCEIP
COOKIEINSERT
SSLSESSION
RULE
URLPASSIVE
CUSTOMSERVERID
DESTIP
SRCIPDESTIP

Increment Interval

Time-out (min)

IPv4 Netmask

IPv6 Mask Length

Loadbalancing algorithm

Persistence required to redirect requests to the same WSA

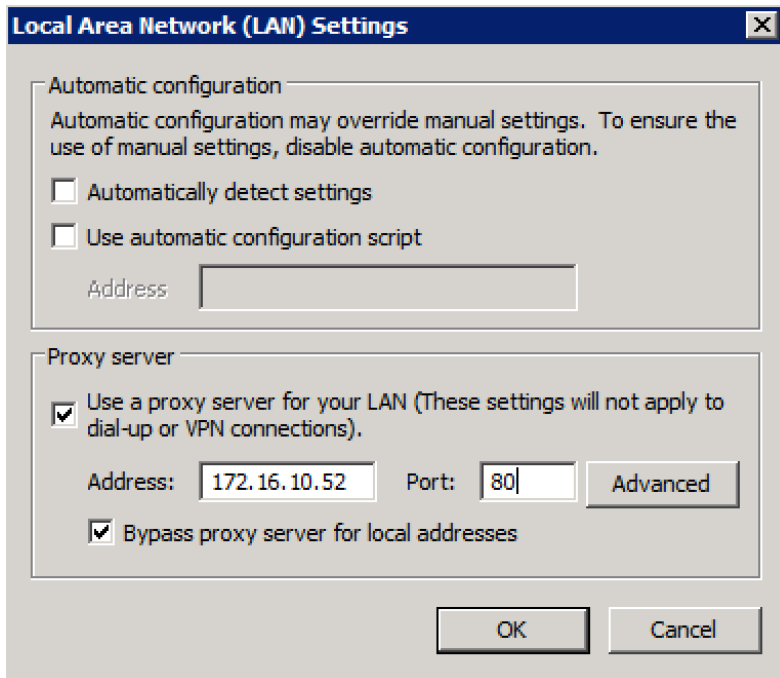


Persistence

- Persistence is required to redirect all requests from a single client to a dedicated WSA
- This is extremely important if you implement your WSA with authentication
 - Example:
Without Persistence, a User might successfully be redirected to WSA1 and authenticated but his next request might end up on WSA3 and authenticated again.
- Using a Loadbalancing Algorithm of URLHASH, DOMAINHASH, DESTINATIONIPHASH or SOURCEIPHASH may remove the need for Persistence
 - All requests from one client would always end up on the same WSA

Netscaler VPX – Browser Settings of the Clients

- Point your Browser to the IP of the Virtual Server



Netscaler VPX – Monitoring

- Easy tracking for Keep-Alive of the Services
- Easy maintenance of proxy systems

Services Graphical View | Default Group

Service(s) Summary

Records per page: 25 | 50 | 100 | 200 1 - 2 of 2

Name	IP address	Port	State	Protocol	Requests	Requests (Rate)	Responses	Responses (Rate)	Request bytes	Request bytes (Rate)
WSA1	172.16.10.45	80	UP	HTTP	1,584	0	1,494	0	1,574,670	0
WSA2	172.16.10.46	80	DOWN	HTTP	0	0	0	0	0	0

Enable Disable

Netscaler VPX – WSA Config

- Enable the WSA to “trust” the Loadbalancer for the “X-Forwarded-for” Header
- This enables the WSA to see the real CLIENT IP in the Access-logs
- IP Address used here is the Netscaler IP Address

Use Received Headers:

Enable Identification of Client IP Addresses using X-Forwarded-For

Trusted Downstream Proxy or Load Balancer

Add Row

172.16.10.51



IP address

Load Balancer Deployment - Summary

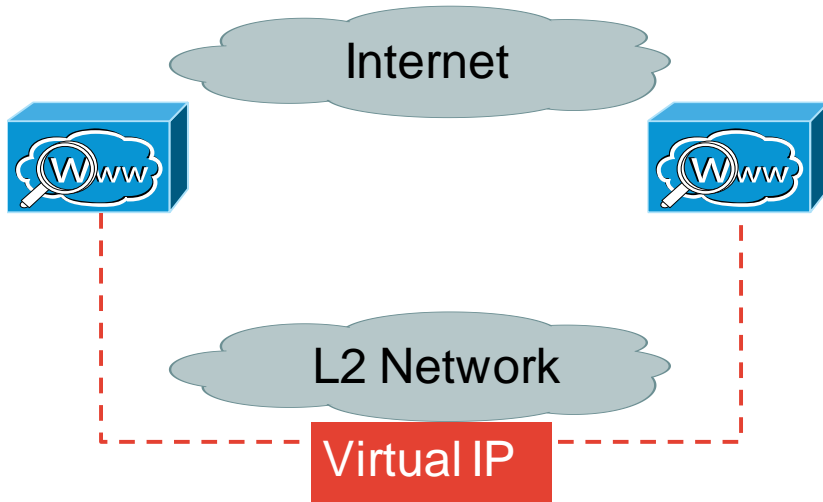
- Netscaler VPX is the virtual Version of the Netscaler Family
- Netscaler can distribute Connections over IPv4 & IPv6
 - Easy way to “enable” your Services with IPv6
- Netscaler settings should be adjusted for “Persistence”
 - Persistence is required to make sure that a certain client is getting all his requests to the same WSA
 - Very Important for authentication!
- Using “X-Forwarded-For” Headers enables the WSA to see the real Client IP in the Access-logs



Deploying with CARP

WSA Redundancy using CARP (1)

Built-in Common Address Redundancy Protocol

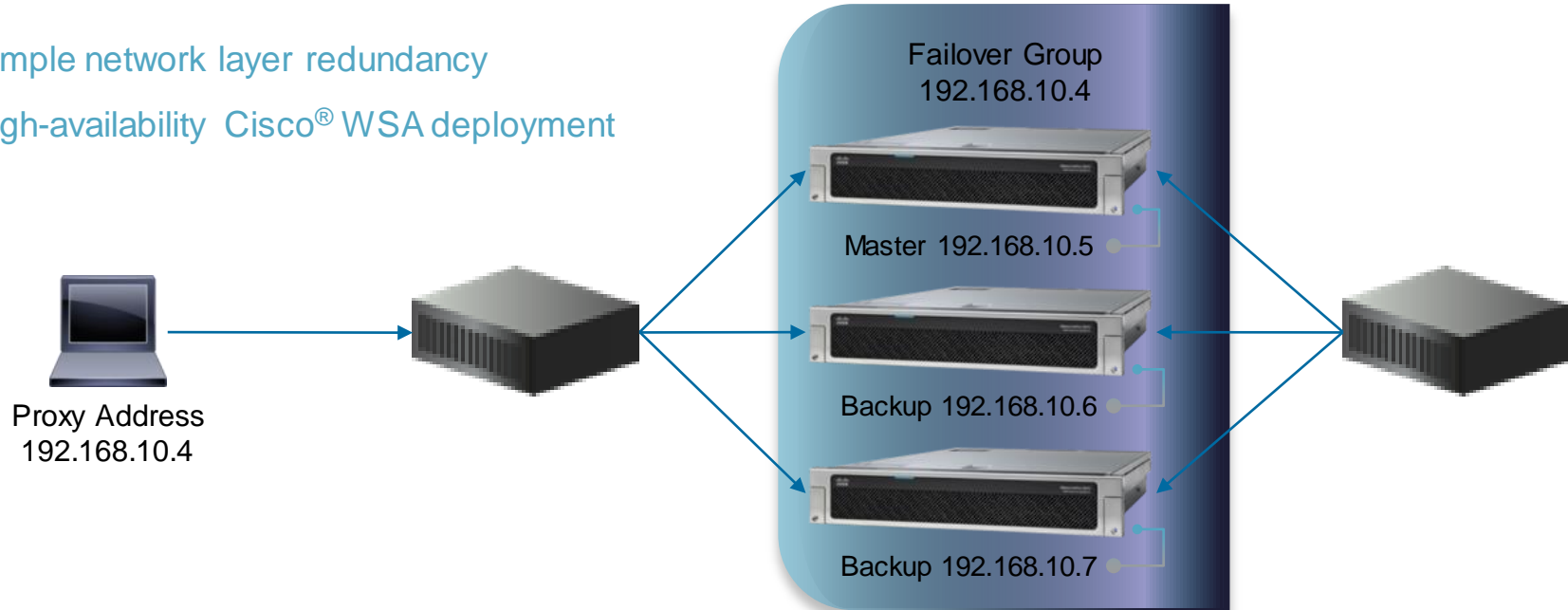


- CARP provides virtual IP
- Works with IPv4 and IPv6
- Requires L2 Connectivity
- Communication done via Multicast
- One Master, multiple Slaves

WSA Redundancy using CARP (2)

Built-in Common Address Redundancy Protocol

- ▶ Simple network layer redundancy
- ▶ High-availability Cisco® WSA deployment





WSA Redundancy using CARP (3)

Built-in Common Address Redundancy Protocol

High Availability

Redundancy Group for IPv4 & IPv6

Failover Groups					
Add Failover Group...					
ID	Hostname	Virtual IP Address/Netmask	Configured Priority	Latest Status	Delete
Failover Group 101	munlab-vwsa-cl.munsec.com	172.16.10.110/24	255	Master (as of 22 October 09:27)	
Failover Group 102	munlab-vwsa1-clv6.munsec.com	2001:420:44e6:2013::110/64	255	Master (as of 22 October 09:27)	

[Refresh Status](#)

High Availability Global Settings	
Failover Handling:	Preemptive (Highest priority server will assume control when online)

[Edit Settings](#)

Configuring CARP

Edit Failover Group: Failover Group 102

Failover Group Settings	
<input checked="" type="checkbox"/> Enable Failover Group	
Failover Group ID:	102 (range 1 through 255)
Description (optional):	v6 failover group
Hostname:	munlab-vwsa1-clv6.munsec
Virtual IP Address and Netmask:	2001:420:44e6:2013::110/64 <small>i.e., 10.0.0.3/24 or 2001:420:80:1::5/3</small>
Interface:	Management <small>If the option Select Interface Automatically is chosen, the interface (ethernet port) will be selected automatically. The virtual IP address must be in the same subnet as the IP address associated with that interface.</small>
Priority: ?	<input checked="" type="radio"/> Master (Priority 255) <input type="radio"/> Backup Priority: <input type="text"/> (range 1 through 254)
Shared Secret for Authentication (optional):	<input type="checkbox"/> Enable Security for Service Shared Secret: <input type="text"/> Retype Shared Secret: <input type="text"/> <small>Provide a shared secret to enable secure communication. The shared value must be the same</small>
Advertisement Interval:	3 sec (range 1 through 255)

Higher Value = Master

Reviewing CARP Configuration

```
munlab-vwsa3.munsec.com> failoverconfig
```

```
Currently configured failover profiles:
```

1. Failover Group ID: 101
Hostname: munlab-vwsa-cl.munsec.com, Virtual IP: 172.16.10.110/24
Priority: 255, Interval: 3 seconds
Status: MASTER
2. Failover Group ID: 102
Hostname: munlab-vwsa1-clv6.munsec.com, Virtual IP: 2001:420:44e6:2013::110/64
Priority: 255, Interval: 3 seconds
Status: MASTER

```
Choose the operation you want to perform:
```

- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)

```
>
```

Troubleshoot Failover Problem

Testing via CLI – “TESTFAILOVERCONFIG”

```
□> TESTFAILOVERGROUP
```

```
Failover group ID to test (-1 for all groups):
```

```
□> -1
```

```
--- Press Ctrl-C to stop ---
```

```
2014/10/22 09:53:25 CARP Out 2001:420:44e6:2013::43 ==> ff02::12 FG Id 102, AdvBase 3 AdvSkew 1(Priority 255)
2014/10/22 09:53:25 CARP Out 2001:420:44e6:2013::43 ==> ff02::12 FG Id 102, AdvBase 3 AdvSkew 1(Priority 255)
2014/10/22 09:53:27 CARP Out 172.16.10.43 ==> 224.0.0.18 FG Id 101, AdvBase 3 AdvSkew 1(Priority 255)
2014/10/22 09:53:27 CARP Out 172.16.10.43 ==> 224.0.0.18 FG Id 101, AdvBase 3 AdvSkew 1(Priority 255)
```

```
^CExiting...
```

```
Stats overview:
```

```
-----
Packets captured:      30
Pkts recv by filter:  32
Pkts drop by kernel:  0
  Connections:        0
  Incomplete Conns:   0
  Total Bytes:         0
  Average Bytes:       0
  Max Bandwidth:       0
  Average Bandwidth:   0
Tracking info 256 buckets: 256 free
-----
```

CARP using mcast for keepalive



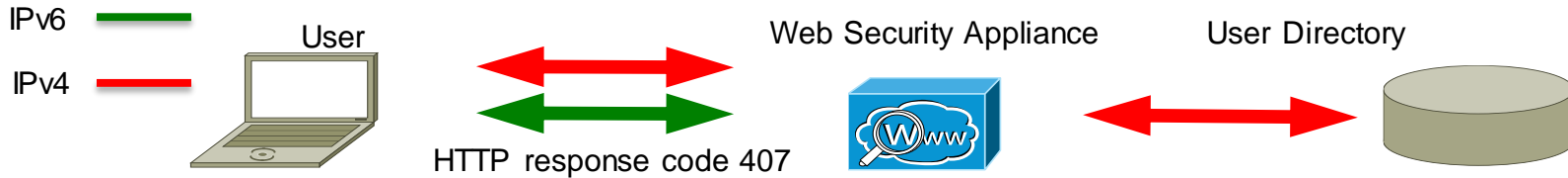
Authentication

Authentication



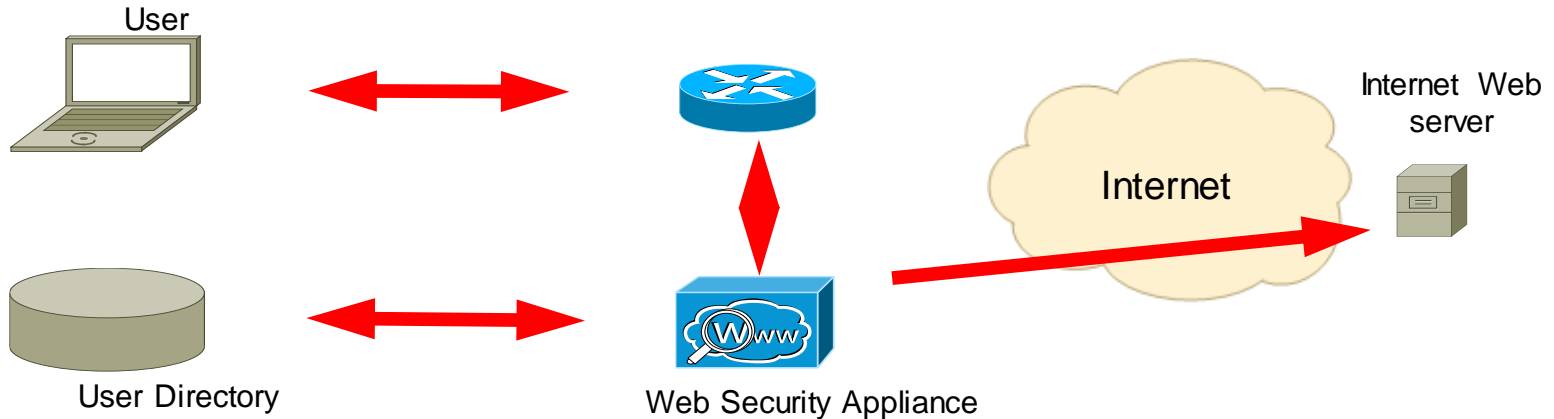
- Authentication Protocols
- Directory:
 - LDAP or Active Directory
- Method:
 - Basic: Credentials are sent unencrypted
 - NTLMSSP: Challenge-Response
 - Kerberos
 - TUI using CDA
- Tracking the User
 - IP based Surrogates
 - Cookie based Surrogates

Authentication in Explicit Deployment



- Proxy sends HTTP response code 407 (proxy auth. request)
 - Client recognises the proxy
 - Client will then accept a http response 407 from the proxy
- Works for HTTPS
 - Client sends a CONNECT request to the proxy
 - Client will then accept a 407 response from the proxy

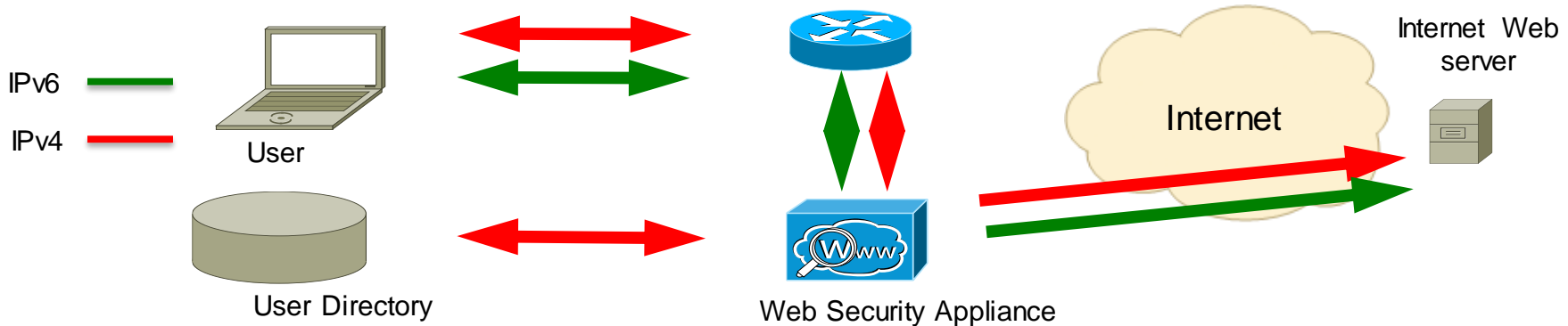
Authentication in Transparent Deployment



- Client is not aware of a proxy -> HTTP response code 407 cannot be used
- Need to use HTTP response code 401
 - Client needs to be first redirected to the wsa
 - Client must trust the „redirect hostname“ when using NTLM to prevent prompting

Authentication in Transparent Deployment

Using Dual Stack



- Client initiates IPv4 (or IPv6) connection in the first packet
- Client is redirected, authenticated and IPv4 (or IPv6) Address stored in wsa
- Client makes another connection, this time using IPv6 (or IPv4)
- Client cannot be found in authentication cache -> needs to authenticate again!

Cisco *live!*

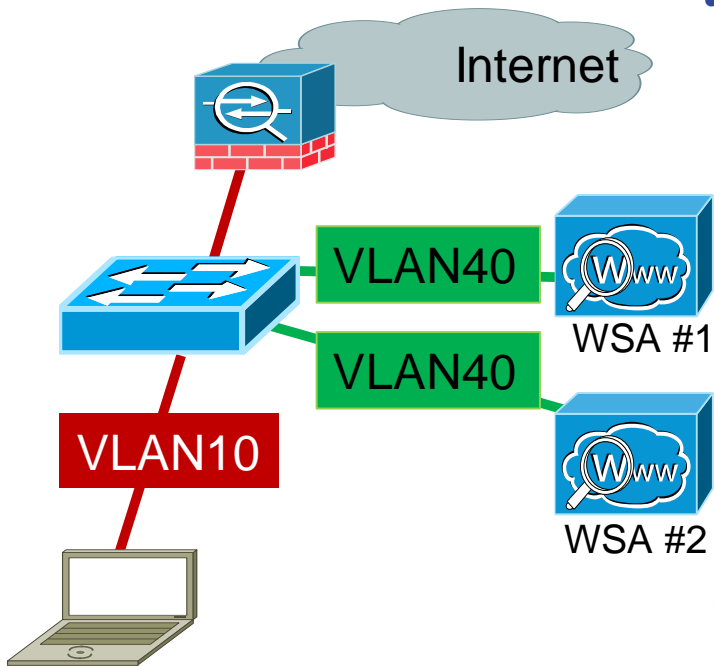
Authentication in Transparent Deployment

Using Dual Stack

- Using NTLM (or Kerberos) & IP Surrogates -> Authenticate twice -> but no problem for User Experience as it is happening in the background
- Using Basic Auth & IP Surrogates -> Authenticate twice
- Using Cookie Surrogates -> Works for IPv4 & IPv6 😊
but: Beware of issues with SSL Traffic!
 - Cookie is inside the SSL Packet and is encrypted.... 😞

WCCP with L3 Switch and Authentication

L2 Redirect, multiple WSA with Auth, avoiding Auth Loop



- First Option:

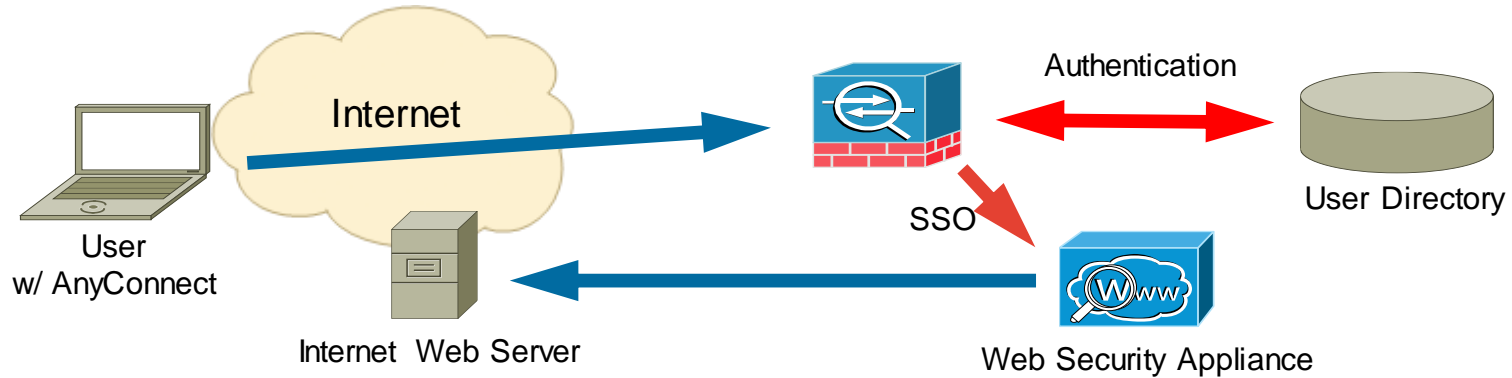
```
ip routing
ip wccp 91 redirect-list wsa
ip access-list extended wsa
!Do not redirect traffic going DIRECTLY to wsa1/2
deny ip any host <wsa1>
deny ip any host <wsa2>
permit tcp any any eq www
permit tcp any any eq 443
!
interface Vlan10
ip address 172.16.10.10 255.255.255.0
ip wccp 91 redirect in
```

- Second Option:

- Load balance based on server address
- Load balance based on client address

Applies only if more than one Web Security Appliance is in use.

Authentication in Secure Mobility Deployment



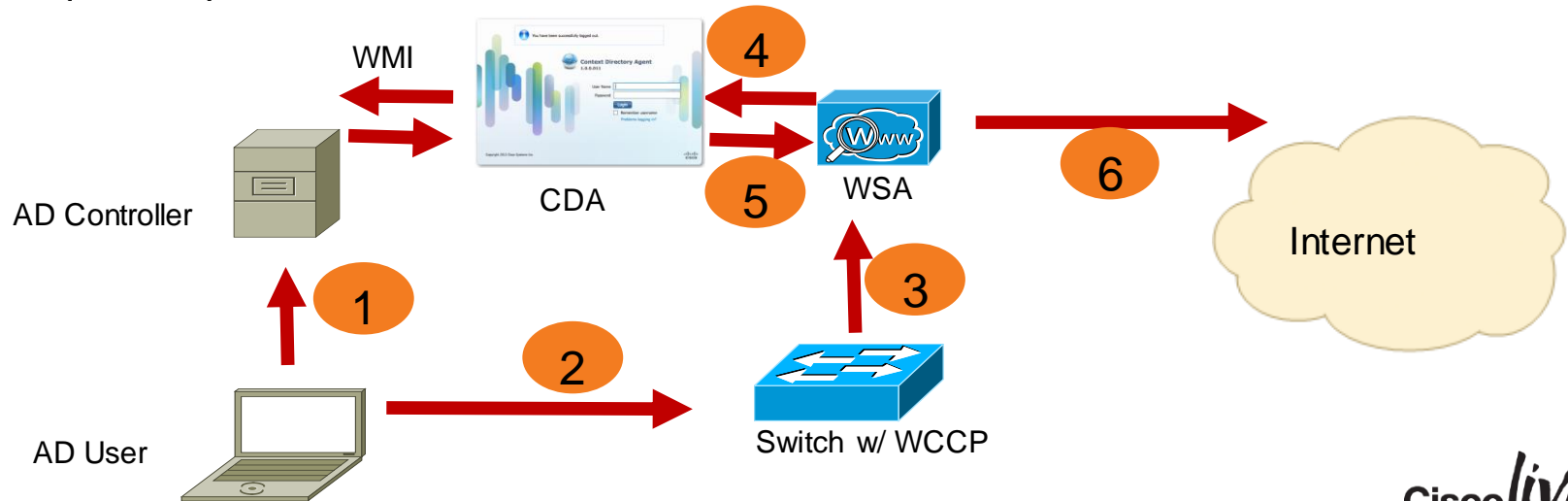
- User connects to ASA via AnyConnect
- ASA authenticates VPN Connection against User Directory
 - After successful authentication, ASA passes user information to WSA for SSO
 - Not dependant on AD-Membership, works for all devices like tablets, phones, etc.
- User can surf via WSA without the need to authenticate again
- WSA can be deployed explicit or transparent

A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.

Transparent User Identification using CDA (Context Directory Agent)

Transparent User Identification (TUI)

1. Client logs on to the AD Domain, CDA tracks AD audit logs and maps User -> IP
2. Client request a Web Site
3. Traffic is transparently redirected to the WSA
4. WSA needs to authenticate and queries the CDA for the User – IP mapping
5. WSA queries AD for User Group
6. Request is proxied and forwarded to the Internet



Context Directory Agent (CDA)

The screenshot displays the configuration status of the Context Directory Agent. It is divided into three main panels:

- Add Active Directory Server:** Shows 1 Domain. Below the domain list is a link for 'Active Directory General Settings'.
- Add Consumer Device(s):** Shows 3 Identity Consumers. Below the list is a link for 'View Registered Devices'.
- Add Syslog Server (Optional):** Shows 0 Syslog Servers. Below the list is a link for 'Log Level Settings'.

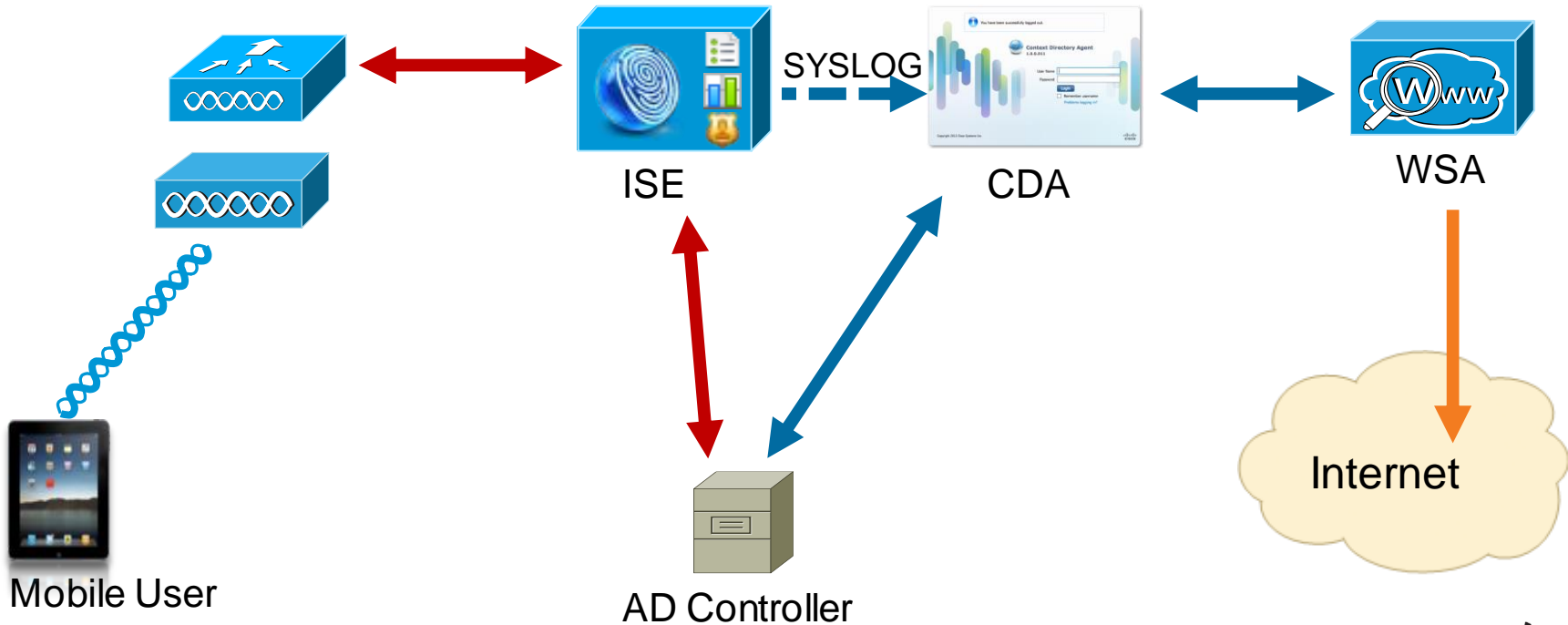
Below the panels are three tables:

- Active Directory Servers:** Total 1. Includes a table with columns for Status and Domain FQDN. One entry is shown: munsec.com.
- Identity Consumers:** Selected 0 | Total 3. Includes a table with columns for Name, IP Address, and Mask. Three entries are shown: munlab-spyker1 (172.16.10.220), munlab-vwsa1 (172.16.10.45), and munlab-wsa01 (172.16.40.100).
- Syslog Servers:** Selected 0 | Total 0. Includes a table with columns for Name, IP Address, and Facility. No entries are shown.

- Linux Image, installed on Virtual Machine
- Getting User-to-IP Mapping (IPv4 & IPv6) via WMI from AD Controller
- Can be queried from WSA, ASA or ASA-CX via Radius

Authentication of Mobile Users Against ISE

...and integration with WSA



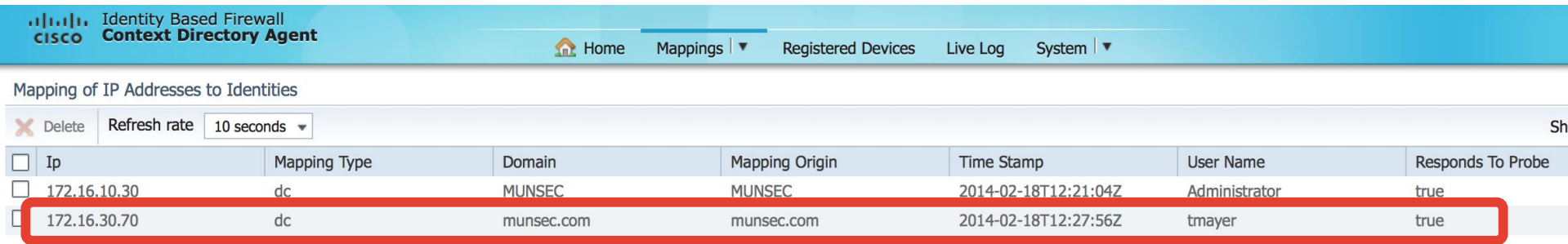
User Authenticates from iPhone to ISE via WLAN

- ISE authenticates the mobile User and gathers information via profiling
- ISE queries AD-Server for Group membership & applies policy

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group
2014-02-18 13:27:56.286			0	tmayer	9C:04:EB:1E:C6:34	Apple-iPhone				
2014-02-18 13:27:45.652				tmayer	9C:04:EB:1E:C6:34	Apple-iPhone	munlab-wlcsec		WLC_FullAccess	Profiled
2014-02-18 11:56:47.671					9C:04:EB:1E:C6:34		munlab-wlcsec			
2014-02-18 11:56:37.162				tmayer	9C:04:EB:1E:C6:34		munlab-wlcsec		WLC_FullAccess	

ISE Sends Radius Updates to CDA

- ISE sends Radius Authentication & Accounting Records to CDA
- Records can be sent via SYSLOG over UDP / SYSLOG over TCP
- CDA adds the mobile User into his USER-IP-Mapping Table



The screenshot shows the Cisco Identity Based Firewall Context Directory Agent interface. The top navigation bar includes 'Home', 'Mappings', 'Registered Devices', 'Live Log', and 'System'. The main content area is titled 'Mapping of IP Addresses to Identities' and features a table with columns for 'Ip', 'Mapping Type', 'Domain', 'Mapping Origin', 'Time Stamp', 'User Name', and 'Responds To Probe'. A red box highlights the second row of the table, which contains the IP address 172.16.30.70, mapping type 'dc', domain 'munsec.com', mapping origin 'munsec.com', time stamp '2014-02-18T12:27:56Z', user name 'tmayer', and 'Responds To Probe' set to 'true'.

Ip	Mapping Type	Domain	Mapping Origin	Time Stamp	User Name	Responds To Probe
172.16.10.30	dc	MUNSEC	MUNSEC	2014-02-18T12:21:04Z	Administrator	true
172.16.30.70	dc	munsec.com	munsec.com	2014-02-18T12:27:56Z	tmayer	true

WSA Transparently Authenticates User Through CDA

Telekom.de 13:34 50 %

Cisco Live Global Events

www.ciscolive.com/ Reader Suchen

Cisco live!

Register today!

Cisco Live 2014, Melbourne, Australia
March 18 - 21, 2014

Welcome to Cisco Live!

Thousands of IT professionals participate in Cisco Live each year. Why? To get the industry's best education. To hear from top experts. To learn about the latest trends and technologies.

Join us and enhance your skills through **global in-person events, live webcasts and on-demand training** focused on Cisco products, solutions and services.

13:29 51 %

ation: Policy: URL Filtering

y.com/ Reader Suchen

ayed

ization's access policies, access to www.playboy.com/) has been

web category "Pornography" is not

please contact your administrator and provide the

Date: Tue, 18 Feb 2014 12:29:21 GMT
Username: MUNSEC.COMtmayer@MUNSEC
Source IP: 172.16.30.70
URL: GET http://www.playboy.com/
Category: Pornography
Reason: BLOCK-WEBCAT
Notification: WEBCAT

WSA – Web Tracking

18 Feb 2014 13:29:21	http://www.playboy.com/ CONTENT TYPE: - URL CATEGORY: Pornography DESTINATION IP: - DETAILS: Access Policy: "PO.MUNSEC". WBRs: 4.2.	Block - URL Cat	0B	MUNSEC.COM\tmayer@MUNSEC (Identified Transparently) 172.16.30.70 Local Access
18 Feb 2014 13:29:14	17.167.195.150:443 (3) CONTENT TYPE: - URL CATEGORY: Computers and Internet DESTINATION IP: 17.167.195.150 DETAILS: Decryption Policy: "DefaultGroup". WBRs: 6.9. ▶ RELATED TRANSACTIONS	Allow	11.2KB	MUNSEC.COM\tmayer@MUNSEC (Identified Transparently) 172.16.30.70 Local Access
18 Feb 2014 13:28:53	http://maps.googleapis.com/maps/api/geocode/json?latlng=48.328137,11.742422&sensor=true CONTENT TYPE: text/plain URL CATEGORY: Search Engines and Portals DESTINATION IP: 173.194.70.95 DETAILS: Access Policy: "PO.MUNSEC". WBRs: 4.9.	Allow	11.8KB	MUNSEC.COM\tmayer@MUNSEC (Identified Transparently) 172.16.30.70 Local Access

TUI – Summary and Caveats

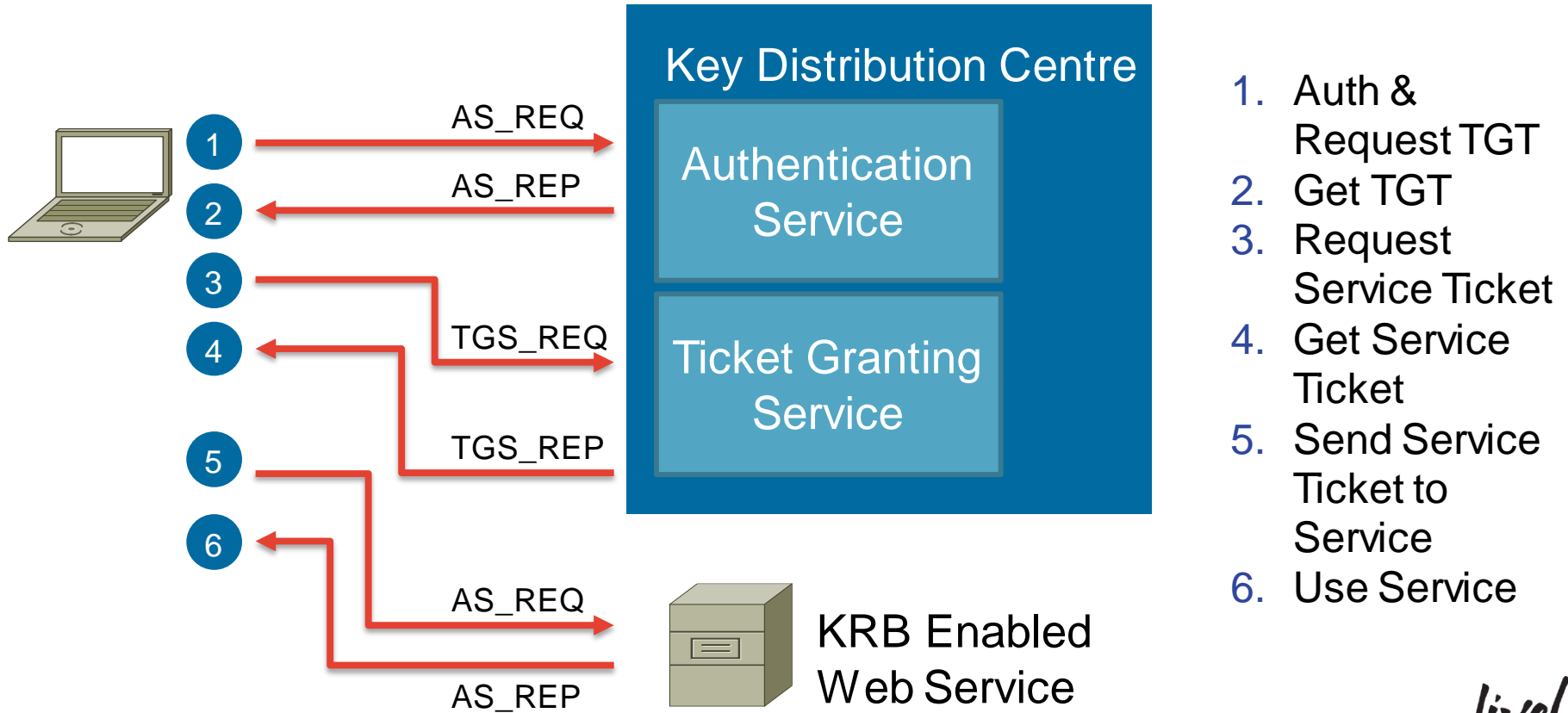
- Uses an Agent (=CDA) running on a Virtual Machine
- Same Agent is also used for Identity based Firewalling on the ASA and ASA-CX
- Allow all applications on the client to work with authentication without starting a browser first
- Does support IPv6 for Client registration and RADIUS messages
 - Privacy extension can cause trouble on clients -> better to disable
- Does not work if Client is NAT-ed after AD Authentication but before reaching the WSA
- Does not work in Terminal Server Environments
- Can receive SYSLOGs from ISE to authenticate mobile devices
 - Provides SSO for mobile Users coming through the WLAN
 - CDA Patch 2 is required

FUTURE: ISE 1.3 PXGRID
Cisco *live!*



Kerberos Authentication

Kerberos – A Quick Refresher



1. Auth & Request TGT
2. Get TGT
3. Request Service Ticket
4. Get Service Ticket
5. Send Service Ticket to Service
6. Use Service

Kerberos and Kerberos Constrained Delegation

- Kerberos Constrained Delegation
 - Kerberos usually requires the client and the KDC to be in the same network
 - In case this is not possible (think of ASA with a clientless SSL Portal), the ASA can request a TGT and Service Ticket on behalf of the client
 - ASA would act as an Authentication Proxy to a “kerberized” application Server in the Backend
- WSA currently supports Kerberos Authentication of clients but **not** Kerberos Constrained Delegation

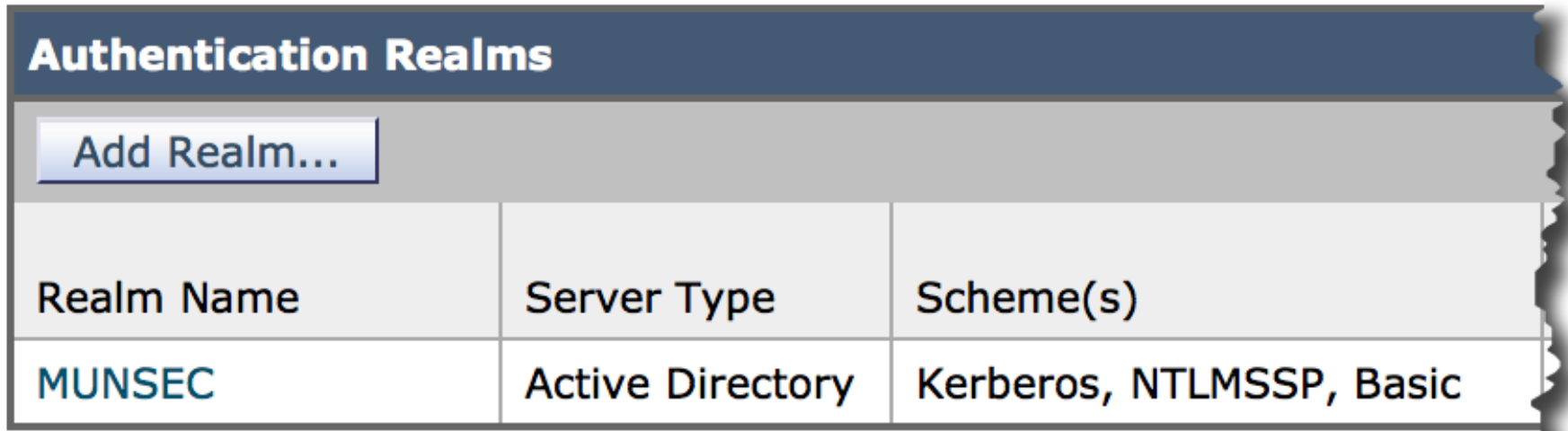
Kerberos vs. NTLM

A simplified view...

- Standard Protocol
 - Available on many platforms (MAC, Linux, Windows, iOS, etc.)
- Preferred Protocol by Microsoft
- Less Resource intense
 - Authentication in one turn
 - Packet is bigger (6-16k)
- Provides SSO for “kerberized” applications
- Client needs to talk to the AD Controller and the Authenticating Server
- Microsoft proprietary
- Legacy protocol
- Mostly on Windows Systems
- More Resource intense
 - Each Server has to authenticate separately with the AD
 - Multiple small packets are exchanged
- Only the Authenticating Server needs to talk to the AD Controller
- Can traverse proxies

Configuration on WSA


- If you upgraded from 7.x to 8.x, re-join the domain
- After re-join, the Kerberos Scheme is available



Realm Name	Server Type	Scheme(s)
MUNSEC	Active Directory	Kerberos, NTLMSSP, Basic

Configuration on WSA (2)


- Edit your Identities to use Kerberos as an authentication Scheme

Select a Realm or Sequence: 

Select a Scheme:

If a user fails authentication:

*Authorization of specific users and groups
(see Web Security Manager > Decryption)*

 Add

MUNSEC

Use Kerberos or NTLMSSP or Basic

Use Kerberos

Use NTLMSSP

Use Basic

Use Kerberos or NTLMSSP

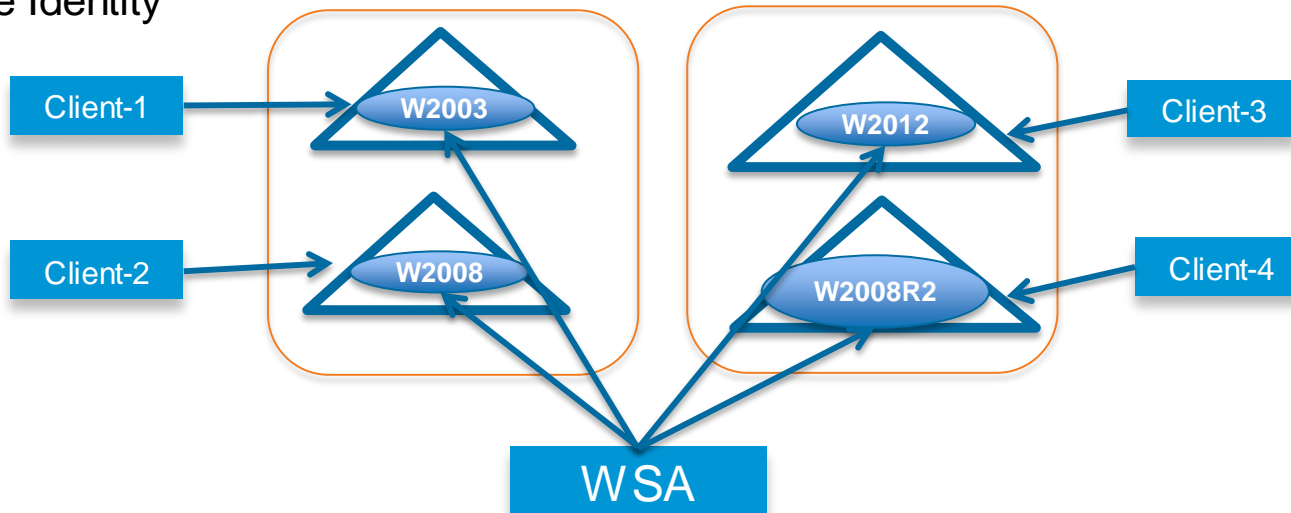
Use Kerberos or Basic

Use NTLMSSP or Basic

Use Kerberos or NTLMSSP or Basic

Multiple Realms within One Identity

- WSA can only use **one** NTLM Realm within one Authentication Sequence
- WSA can use **multiple** Kerberos Realms in one Authentication Sequence
 1. Create each Realm on the WSA
 2. Create a sequence on all the Realms
 3. Create Identity



Configuration on WSA (3)

- Strongly recommended to add %m to the accesslog (=Authentication Method)



- **BASIC.** The user name was authenticated using the Basic authentication scheme.
- **NTLMSSP.** The user name was authenticated using the NTLMSSP authentication scheme.
- **NEGOTIATE.** The user name was authenticated using the KERBEROS authentication scheme.
- **SSO_TUI.** The user name was obtained by matching the client IP address to an authenticated user name using transparent user identification.
- **SSO_ASA.** The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility.
- **FORM_AUTH.** The user entered authentication credentials in a form in the web browser when accessing a application.
- **GUEST.** The user failed authentication and instead was granted guest access.

Quick Test from a MAC

Request a Ticket from the
Kerberos Domain
"MUNSEC.COM"

```
tmayer — bash —
Last login: Mon Mar 10 10:29:53 on console
tmayer-mac:~ tmayer$ klist
klist: krb5_cc_get_principal: No credentials cache file found
tmayer-mac:~ tmayer$ kinit tmayer@MUNSEC.COM
tmayer@MUNSEC.COM's Password:
tmayer-mac:~ tmayer$ klist
Credentials cache: API:501:1
Principal: tmayer@MUNSEC.COM
```

Issued	Expires	Principal
Mar 10 10:32:06 2014	Mar 10 20:32:05 2014	krbtgt/MUNSEC.COM@MUNSEC.COM

TGT is displayed

Quick Test from a MAC (2)

- After requesting access from the WSA we got a Service Ticket for the WSA

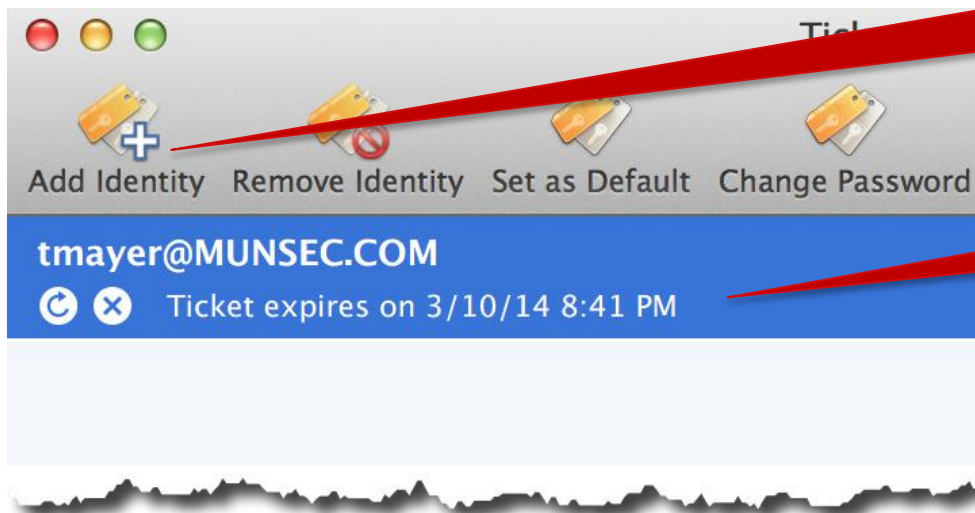
```
tmayer-mac:~ tmayer$ klist
Credentials cache: API:501:3
Principal: tmayer@MUNSEC.COM

Issued                        Expires                        Principal
Mar 10 10:41:08 2014      Mar 10 20:41:08 2014      krbtgt/MUNSEC.COM@MUNSEC.COM
Mar 10 10:42:01 2014      Mar 10 20:41:08 2014      HTTP/munlab-wsa1@MUNSEC.COM
tmayer-mac:~ tmayer$
```

Service Ticket for access to the
WSA

Quick Test from a MAC (3)

- /System/Library/CoreServices/Ticket Viewer

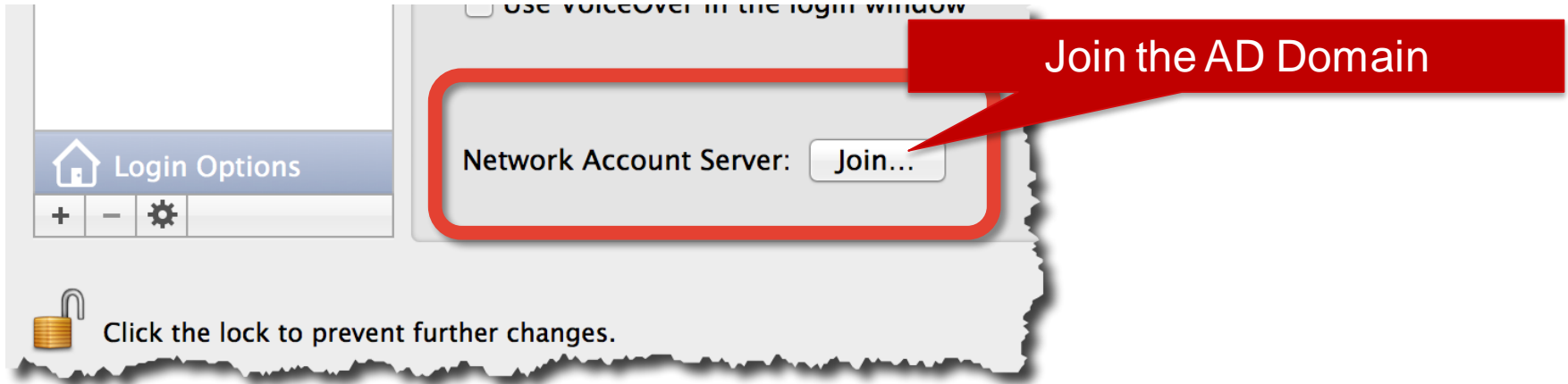


Request a Ticket from the Kerberos Domain MUNSEC.COM

TGT is displayed

Example #1 : Join the AD Domain with Your MAC

- Joining the MAC to the AD Domain will create a computer account on the AD Server



- After successful join, log out and log in again with your AD Account
- When opening Safari, you will get authenticated to the WSA without prompt 😊
- http://training.apple.com/pdf/wp_integrating_active_directory_ml.pdf

Kerberos Authentication with WCCP

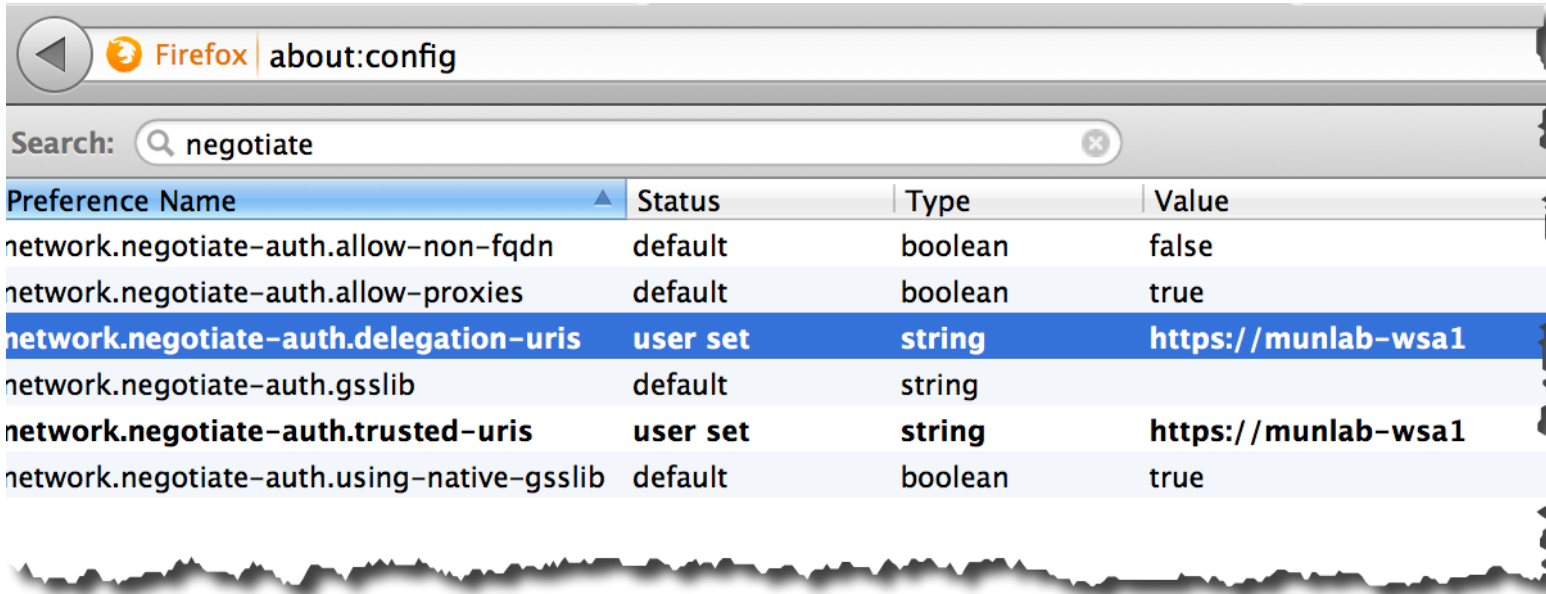
- When using transparent redirection and Kerberos, non-windows Clients like MAC OS X sometimes have problems with the redirection
- Make sure the WSA Hostname is the same than the redirection name

Authentication Settings	
Credential Encryption:	Disabled
Redirect Hostname:	munlab-wsa1.munsec.com
Credential Cache Options:	Surrogate Timeout: 3600 seconds

- WSA only accepts FQDN as Hostname ☹️ -> Redirection Name as FQDN might cause trouble with Windows Clients
 - Windows Clients require the redirection hostname added to the “Intranet Zone”

Firefox Config for Kerberos

- Add the WSA as a trusted URL for Kerberos when prompted:



The screenshot shows the Firefox 'about:config' page with a search for 'negotiate'. The table below lists several preferences, with 'network.negotiate-auth.delegation-uris' highlighted in blue, indicating it is user-set to 'https://munlab-wsa1'.

Preference Name	Status	Type	Value
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	user set	string	https://munlab-wsa1
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	user set	string	https://munlab-wsa1
network.negotiate-auth.using-native-gsslib	default	boolean	true

Debugging on the AD Server

- Turn on debugging on the AD Server for Kerberos
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
 - Set “LogLevel” to “1” / Set “LogLevel” to “0” de-activates Kerberos debugging
- Windows Events
 - 4768 : A TGT Ticket was Requested
 - 4769: A Kerberos Service Ticket was Requested
 - Both Events log success and failures. Result Codes: <https://www.ietf.org/rfc/rfc4120.txt>
- Check on AD-Server if SPN from WSA have been registered:

```
C:\Users\Administrator>setspn -l MUNLAB-WSA1
Registered ServicePrincipalNames for CN=MUNLAB-WSA1,CN=Computers,DC=munsec,DC=co
m:
    HTTP/munlab-wsa1.munsec.com
    HOST/munlab-wsa1.munsec.com
    HTTP/MUNLAB-WSA1
    HOST/MUNLAB-WSA1
```


Kerberos - Summary

- WSA can authenticate users using Kerberos
 - Need to re-join the Domain if the “Kerberos” scheme is not displayed
- Windows Clients will automatically try Kerberos first then fall back to NTLM
- Modify your accesslog with the “%m” Parameter to check the authentication method
- Enables Users to authenticate with non-windows clients like MAC, LINUX or iOS 7.0 (iphone, ipad)
 - iOS 7 Enterprise SSO is best configured using a MDM (Mobile Device Manager)
- Authenticate once and use ticket for multiple sites
 - Useful when using several WSA such as with a load balancer

A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, modern city buildings are illuminated with various lights, and a pedestrian bridge spans across the street. The overall scene is a dynamic urban environment.

Advanced Malware Protection (AMP)

Advanced Malware Protection (AMP)

- AMP is a separate License consisting of:
 - File Reputation
 - File Analysis
- After it is enabled, include it in the access policies just like any other scanner

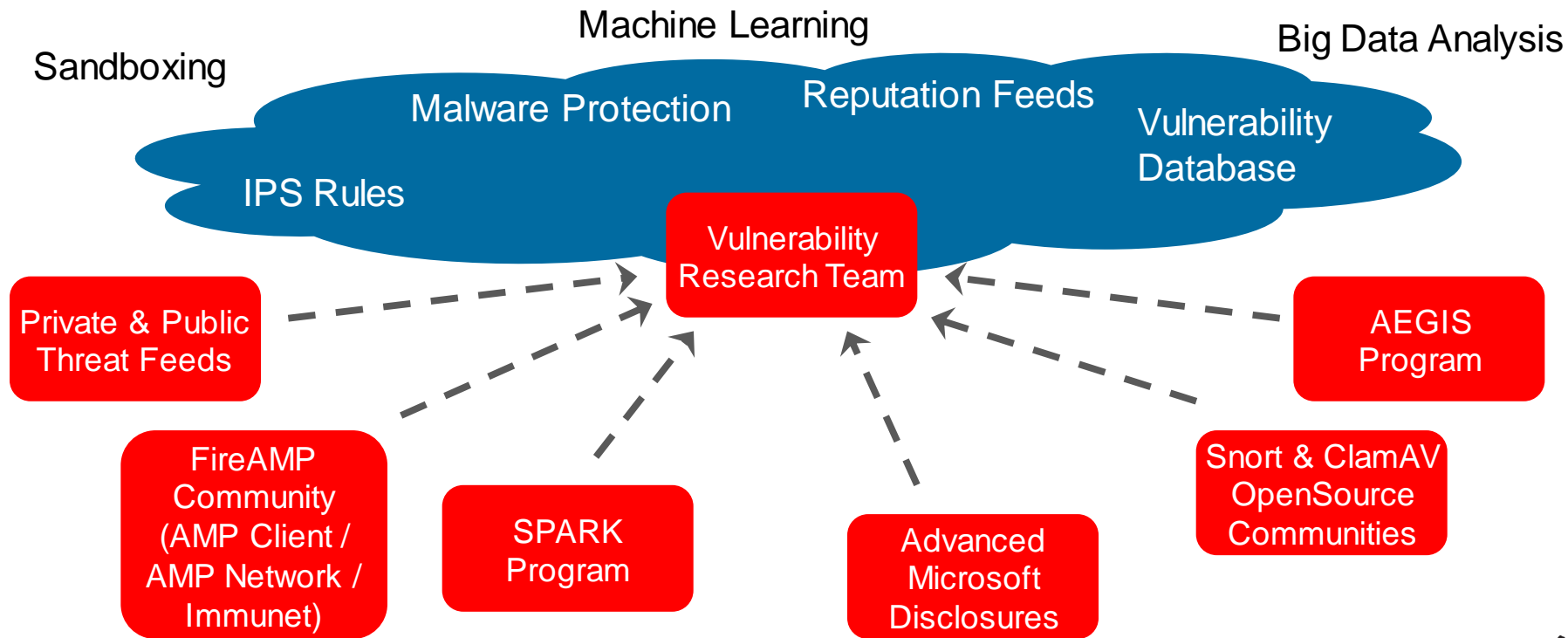
Anti-Malware and Reputation Settings	
Reputation Services	
Web Reputation Filtering:	Enabled
Adaptive Scanning:	<i>Adaptive Scanning is currently disabled globally.</i>
Advanced Malware Protection Services	
File Reputation Filtering:	Enabled
File Analysis:	Enabled
Anti-Malware Scanning Services	

Advanced Malware Protection (AMP)

3	PO.FALCONLAB Identity: ID.FALCONLAB	(global policy)	(global policy)	Block: 1 Restrict: 1 Monitor: 216	(global policy)	Web Reputation: Disabled Advanced Malware Protection: Enabled Webroot: Enabled Sophos: Enabled
---	---	-----------------	-----------------	---	-----------------	--

- File Reputation
 - Ability to create a SHA-256 Hash of the file and check against the cloud database
 - Cloud delivers back a Verdict consisting of “malicious”, “unknown” or “clean”
 - File Reputation is available for high risk file types such as “.EXE”, “.ZIP”, “.PDF”, etc
- File Analysis
 - Optional upload of Files into the cloud for dynamic analysis
 - Delivers back a Verdict Score (0-100)
 - Score above 60 is considered “malicious”
- Ports required from WSA to AMP Cloud: tcp/443 and tcp/32137 (over M1)

Vulnerability Research Team (VRT)



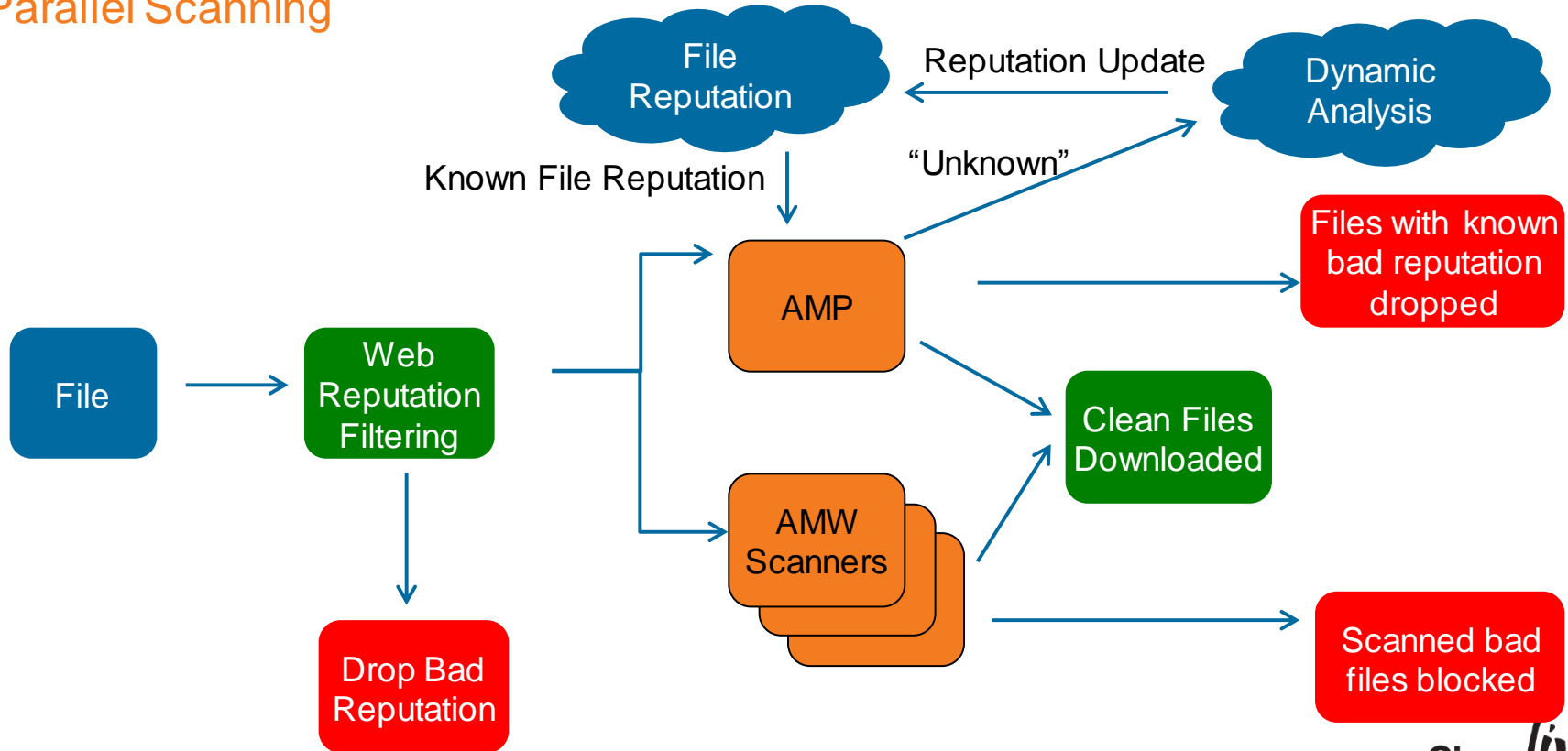
Advanced Malware Protection (AMP) - SPERO

File Reputation

- When the SHA-256 is calculated from a file, we also calculate a “Featureprint” of the PE-Headers
 - Some examples are DLLS_REFERED, Optional Headers (standard and windows), data sections
- Featureprint is sent to the cloud alongside the SHA-256
- It is analysed using Big Data Analytics and machine learning
 - Are the PE Header Values similar to those found in known malware?
 - Are the PE-Headers trying to call suspicious DLLs?
 - ...
- This is just one of many mechanism used to detect new and unknown malware

Advanced Malware Protection (AMP)

Parallel Scanning



File Analysis– What Can Be Analysed By The Cloud?

The following criteria must be met to upload the file for analysis

- File is a windows executable, for example .exe, .dll, .scr or .sys
 - Needs to contain PE Headers
- File Size is less than 1 MB
- Only Files downloaded are analysed,
 - file uploads are not analysed
- Capabilities will be enhanced in following releases

AMP – Global Settings

Enable File Reputation Filtering

Enable File Analysis

When File Analysis is enabled, files may be automatically sent to the cloud for further analysis. This provides the highest and targeted threats. File Analysis is only available when file reputation filtering is enabled.

Cloud Domain:

Cloud Server Pool:

Heartbeat Interval: seconds

Reputation Threshold:
valid range 1 through 100, recommended value 60

Query Timeout: seconds

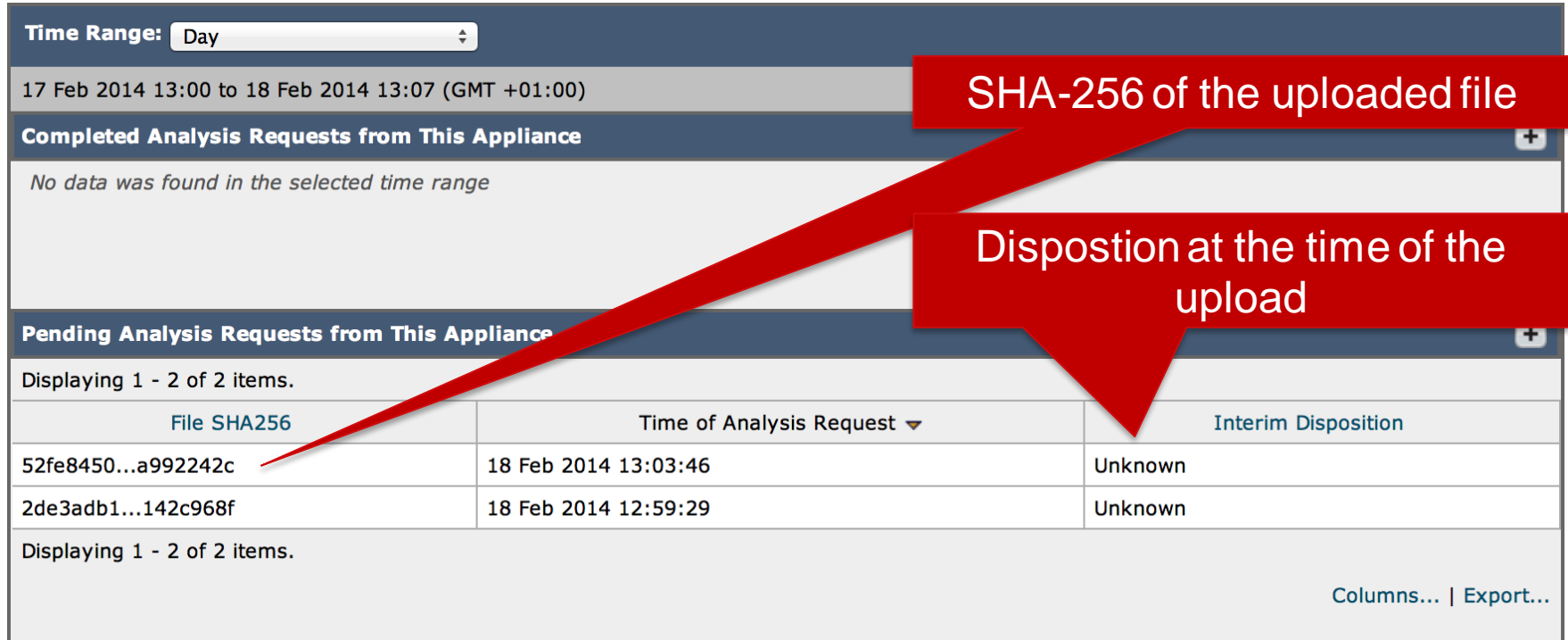
File Analysis Server URL:

Client ID (Reference Only):
File Reputation: f6eb4487-9abc-4c75-b937-fab3c6f32c78
File Analysis: 02564c4e575341313438323837230000000000

Threshold when the “Verdict” is considered as malicious

AMP – Files Analysed in the Cloud

Files uploaded and Pending Analysis – Disposition “Unknown”



Time Range: Day

17 Feb 2014 13:00 to 18 Feb 2014 13:07 (GMT +01:00)

Completed Analysis Requests from This Appliance

No data was found in the selected time range

Pending Analysis Requests from This Appliance

Displaying 1 - 2 of 2 items.

File SHA256	Time of Analysis Request	Interim Disposition
52fe8450...a992242c	18 Feb 2014 13:03:46	Unknown
2de3adb1...142c968f	18 Feb 2014 12:59:29	Unknown

Displaying 1 - 2 of 2 items.

[Columns...](#) | [Export...](#)

SHA-256 of the uploaded file

Disposition at the time of the upload

AMP – Files Analysed in the Cloud(2)

Disposition “Clean”

Time Range:

17 Feb 2014 14:00 to 18 Feb 2014 14:02 (GMT +01:00)

Completed Analysis Requests from This Appliance +

Displaying 1 - 2 of 2 items.

File SHA256	Time of Analysis Request	Time Analysis Completed ▼	Disposition
1fb0c254...4263c92e	18 Feb 2014 13:22:09	18 Feb 2014 13:25:48	Clean
bfacb9e7...17ab16cb	18 Feb 2014 13:22:12	18 Feb 2014 13:25:43	Clean

Displaying 1 - 2 of 2 items.

[Columns...](#) | [Export...](#)

Pending Analysis Requests from This Appliance +

No data was found in the selected time range

File was analysed and considered as “clean”

AMP – Files Analysed in the Cloud(3)

Disposition “Malicious”

Time Range: 30 days

19 Jan 2014 00:00 to 18 Feb 2014 12:24 (GMT +01:00)

Completed Analysis Requests from This Appliance +

Displaying 1 - 2 of 2 items.

File SHA256	Time of Analysis Request	Time Analysis Completed ▾	Disposition
c9b4d4ab...069746ac	11 Feb 2014 14:39:34	11 Feb 2014 14:46:39	Malicious
53de8225...143d024d	11 Feb 2014 14:25:43	11 Feb 2014 14:29:47	Malicious

Displaying 1 - 2 of 2 items.

[Columns...](#) | [Export...](#)

Pending Analysis Requests from This Appliance +

No data was found in the selected time range

AMP – Verdict Changes

Disposition was “Unkown” and changed to “Malware”

Advanced Malware Protection Verdict Updates

[Printable \(PDF\)](#)

Time Range:

11 Feb 2014 00:00 to 18 Feb 2014 11:06 (GMT +01:00)

Files with Retrospective Verdict Changes +

File SHA256	Time of Retrospective Verdict Change	Current Disposition
c9b4d4aba893f0...dcde8b069746ac	14 Feb 2014 07:05:14	Malware
53de8225fc823c...05d8e3143d024d	14 Feb 2014 07:05:14	Malware

[Columns...](#) | [Export...](#)

[Link to Detailed Analysis](#)

AMP – Detailed Analysis

File Analysis Detail > 53de8225fc823c...05d8e3143d024d

[Printable \(PDF\)](#)

General Information	
Analysis ID:	17445761
Start time:	13:29:44
Start date:	2014-02-11
Number of analysed new started processes:	4
Score:	100
Status:	Complete

[Export...](#)

Classification / Threat Score		
Factor	Score	Threat Level
AV Detection	1	Low
Networking	1	Low
Persistence and Installation Behavior	100	Very High
PE File Obfuscation	6	Low
System Summary	39	Medium
HIPS / PFW / Operating System Protection Evasion	95	Very High
Anti Debugging	63	High
Virtual Machine Detection	14	Low
Language and Operating System Detection	1	Low

Cisco *live!*

AMP – Detailed Analysis (2)

Matching Signatures	
	Items Displayed 10
Signatures	
VirusTotal Search Results	
Urls found in memory or binary data	
Drops PE files	
Binary may include packed or crypted data	
PE file contains sections with non-standard names	
PE sections with suspicious entropy found	
Creates temporary files	
Executable uses VB runtime library 6.0 (Probably coded in Visual Basic)	
Reads ini files	
Spawns processes	

[Export...](#)


Static File Info	
MD5:	9FB9F6A06A41EFE0CFA1EAA76106AEC4
SHA1:	6DE00EC3BBC9D512919A45712B0E8DBA383C0795
SHA256:	53DE8225FC823C6EFC8AD33A3A741FBE4C56B041EF51E4D70605D8E3143D024D

AMP – Check Web Tracking

Static File Info

MD5:	BB03F36B09E1ACF98284489524DFCF3A
SHA1:	67868E86FF6122746777FE83F395EEBCB6F1B8F5
SHA256:	C9B4D4ABA893F0675E7CE34C812834452C6267D3DEABB89398DCDE8B069746AC

[Export...](#)

To view all transactions for this threat, see: [Web Tracking for SHA256 c9b4d4aba893f0675e7ce34c812834452c6267d3deabb89398dcde8b069746ac](#)
To view full analysis details in the cloud, see: [Cisco Sourcefire Threat Analysis](#) 

AMP – Drill Down into Web Tracking

Web Tracking

Search

Proxy Services | **L4 Traffic Monitor** | **SOCKS Proxy**

Available: 22 Oct 2013 13:44 to 13 Feb 2014 15:10 (GMT +01:00)

Time Range:

User/Client IPv4 or IPv6: (e.g. jdoe, DOH, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type:

Advanced *Current Criteria: File SHA256: 53de8225fc823c6efc8ad33a3a741fbe4c56b041ef51e4d70605d8e3143d024d.*

SHA-256

Users and IPs that have downloaded the file

Generated: 18 Feb 2014 11:02 (GMT +01:00)

Results

Displaying 1 - 3 of 3 items.

Time (GMT +01:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
11 Feb 2014 14:49:59	http://batcoroadlinescorporation.com		Allow	116.7KB	sales fd00:1:2:3::1
11 Feb 2014 14:32:44	http://batcoroadlinescorporation.com		Allow	116.7KB	sales fd00:1:2:3::1
11 Feb 2014 14:25:41	http://vistatech.us		Allow	116.5KB	sales fd00:1:2:3::1

Displaying 1 - 3 of 3 items.

AMP – Granular Report from Sourcefire Cloud

VRT Analysis Report Overview Startup Dropped Domains / IPs Static Network Hooks Behavior ▾

PE File Obfuscation:

- Binary may include packed or encrypted data
- PE file contains sections with non-standard names
- PE sections with suspicious entropy found

System Summary:

- Creates temporary files**
Source: C:\17445761.exe | File created: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsoD.tmp
- Executable uses VB runtime library 6.0 (Probably coded in Visual Basic)**
Source: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\hwsbymvk.exe | Section loaded: C:\WINDOWS\system32\msvbvm60.dll
- Reads ini files**
- Spawns processes**
- Creates files inside the system directory**
Source: C:\WINDOWS\system32\wbem\wmiprvse.exe | File created: C:\WINDOWS\system32\WBEM\Logs\FrameWork.log
- Enables driver privileges**
- Tries to load missing DLLs**



Accesslog - New Fields

```
1392726116.910 2969 2001:420:44e6:2013::30 TCP_MISS/200 520698 GET
http://tartarus.org/~simon/putty-snapshots/x86/putty.exe
"MUNSEC\administrator@MUNSEC" DIRECT/tartarus.org application/x-dosexec
DEFAULT_CASE_12-PO.MUNSEC-ID.MUNSEC-NONE-NONE-NONE-
DefaultGroup <IW_busi,-5.8,0,"-",0,0,0,-,"-",-,-,"-",0,0,"-","-",-,-,IW_busi,-
,"Unknown","othermalware","Unknown","Unknown","-","-
",1403.03,0,Local,"Unknown","-",0,"-
",8,0,"putty.exe","2de3adb1f57e05a0f07c9a9f50ead4df7e6374e215d87329baab02
8b142c968f"> - DestIP: 80.252.125.10NTLMSSP
```



Return Code (0=Clean)



File requested to be uploaded for analysis? (0=not req)



Threat Name



Filename



Threat Verdict Code



SHA-256 of the File

Accesslog - Example for Malicious File

SHA-256 is known as malicious to the Cloud

```
1392125769.465 1704 fd00:1:2:3::1 TCP_DENIED/403 0 GET
http://valouweeigenaren.nl/customers/billing/df367548-18.zip
"sales@FALCONLAB" DIRECT/valouweeigenaren.nl application/zip
BLOCK_AMP_RESP_12-PO.FALCONLAB-ID.FALCONLAB-NONE-NONE-NONE-
DefaultGroup <nc,-6.9,-,"-",-,-,1,"-",-,-,"-",-,-,"-",-,-,nc,-,"AMP High
Risk","othermalware","Unknown","Unknown","-","-",0.00,0,Local,"-","-
",37,"BBGG:Trojan3-tpd",0,0,"df367548-
18.zip","ce3fbaa76e6424832bf759b51ddd08018f2c567e1f6016aeb8938eecb05d6
3dd"> -
```



Return Code (0=Clean)



Threat Name



Threat Verdict Code



File requested to be uploaded for analysis? (0=not req)

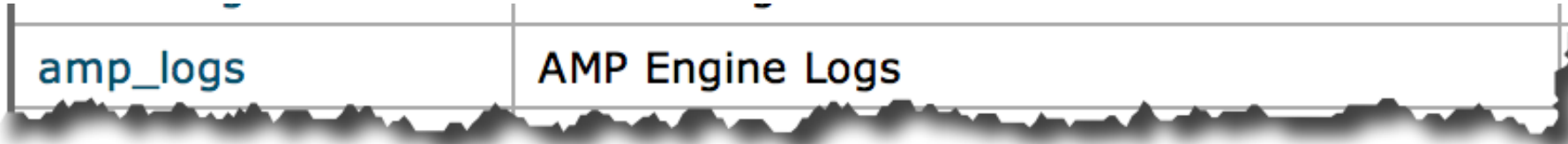


Filename



SHA-256 of the File

AMP – Logfiles (amp_log)



- File was uploaded to the cloud:

```
Tue Feb 11 14:39:34 2014 Info: amp File uploaded for analysis. SHA256:  
c9b4d4aba893f0675e7ce34c812834452c6267d3deabb89398dcde8b069746ac, Timestamp:  
1392125974
```

AMP – Logfiles (amp_log)

- File was analysed and verdict delivered back to the appliance

```
Tue Feb 11 14:53:12 2014 Info: amp Sandbox status event received - {"runs":[{"runid":  
17445761,"date":"2014-02-11T13:25:44Z","status":"Complete","sample":  
{"SHA1":"6DE00EC3BBC9D512919A45712B0E8DBA383C0795","SHA256":"53DE8225FC823C6EFC8AD33A3A7  
41FBE4C56B041EF51E4D70605D8E3143D024D","MD5":"9FB9F6A06A41EFE0CFA1EAA76106AEC4"},"score"  
:100,"platform":{"arch":"i386","os":"Windows XP -  
SP3"},"updated":"2014-02-11T13:29:47Z"}],"total":1}, SHA:  
53de8225fc823c6efc8ad33a3a741fbe4c56b041ef51e4d70605d8e3143d024d  
Tue Feb 11 14:53:12 2014 Warning: amp Sandbox file analysis complete. SHA256:  
53de8225fc823c6efc8ad33a3a741fbe4c56b041ef51e4d70605d8e3143d024d, Submit Timestamp:  
1392125143, Update Timestamp: 1392125387, trr: 0, run_id: 17445761  
Tue Feb 11 14:53:13 2014 Info: amp Sandbox status event received - {"runs":[{"runid":  
17447029,"date":"2014-02-11T13:39:35Z","status":"Complete","sample":  
{"SHA1":"67868E86FF6122746777FE83F395EEBCB6F1B8F5","SHA256":"C9B4D4ABA893F0675E7CE34C812  
834452C6267D3DEABB89398DCDE8B069746AC","MD5":"BB03F36B09E1ACF98284489524DFCF3A"},"score"  
:100,"platform":{"arch":"i386","os":"Windows XP -  
SP3"},"updated":"2014-02-11T13:46:39Z"}],"total":1}, SHA:  
c9b4d4aba893f0675e7ce34c812834452c6267d3deabb89398dcde8b069746ac  
Tue Feb 11 14:53:13 2014 Warning: amp Sandbox file analysis complete. SHA256:  
c9b4d4aba893f0675e7ce34c812834452c6267d3deabb89398dcde8b069746ac, Submit Timestamp:  
1392125974, Update Timestamp: 1392126399, trr: 0, run_id: 17447029
```

AMP – Logfiles (amp_log)

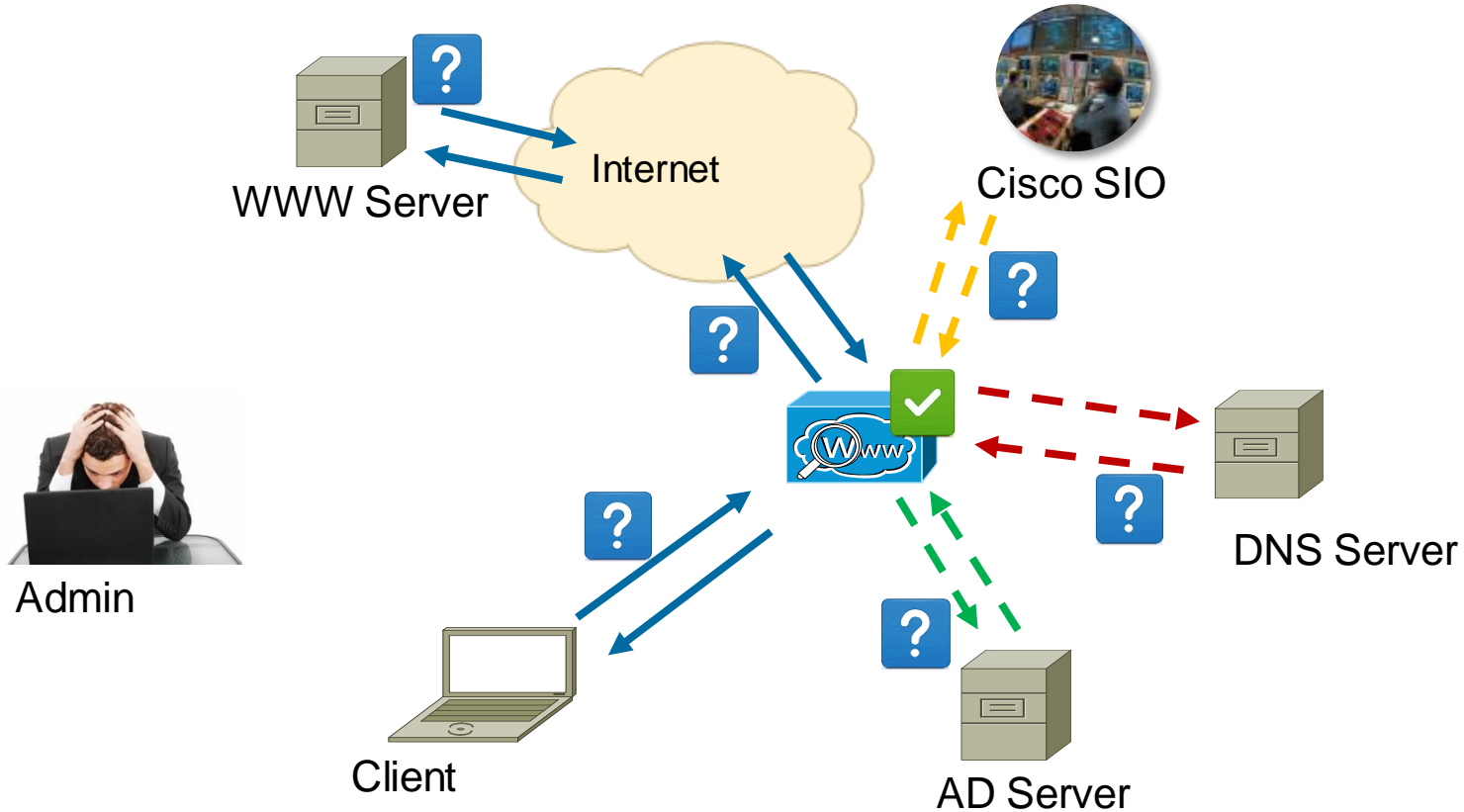
- WSA cannot reach the Cloudservice
 - Check connectivity on required ports (tcp/443 and tcp/32137)

```
Sun Feb 16 22:29:45 2014 Warning: amp The file reputation service in the cloud is unreachable. Event: AMP_ASYNC_EVENTS.CLOUD_UNREACHABLE
```



Troubleshooting Performance Issues

WSA Performance Analysis




Debugging Performance issues

- Download file “prox_track.log” from appliance via FTP
- File is written every 5 minutes with timestamp

Setting can be changed in „advancedproxyconfig“ on CLI

Index of ftp://munlabwsa/track_stats/

 [Up to higher level directory](#)

Name	Size	Last Modified	
 README	1 KB	4/23/08	12:00:00 AM
 prox_track.log	886 KB	10/31/12	11:18:00 AM
 prox_track.log.1.gz	1739 KB	10/30/12	9:00:00 AM
 prox_track.log.2.gz	1735 KB	10/29/12	9:00:00 AM
 prox_track.log.3.gz	1733 KB	10/28/12	9:00:00 AM
 prox_track.log.4.gz	1734 KB	10/27/12	10:00:00 AM
 prox_track.log.5.gz	1730 KB	10/26/12	10:00:00 AM
 prox_track.log.0.gz	1741 KB	10/31/12	9:00:00 AM

Prox_track.log Content

- Contains various statistical data around proxy performance
- Please do NOT consider all number of packets 100% accurate!
- Just gives a good hint what problem might be happening

```
Oct 31 09:00:01 munlabwsa newsyslog[62539]: logfile turned over due to size>10000K

Current Date: Wed, 31 Oct 2012 09:02:15 CET
      user time: 0.173
      system time: 0.032
      max resident set size: 0
      integral sh'd text mem size: 6580
      integral unshared data size: 244328
      integral unshared stack size: 4480
      page reclaims: 0
      page faults: 0
      swaps: 0
      block input operations: 1
      block output operations: 0
      messages sent: 26
      messages received: 29
      signals received: 0
      voluntary context switches: 5082
      involuntary context switches: 268
      INFO: prox running for 10175 minutes
```

General Statistics

- Traffic Statistics:

If you have numbers increasing on “throttled transactions” this could indicate that the appliance can not handle the load

```
INFO: traffic over past minute - 0.00 reqs/sec
INFO: traffic over past hour - 0.52 peak / 0.06 avg reqs/sec
INFO: traffic over past day - 1.32 peak / 0.01 avg reqs/sec
INFO: traffic over past week - 2.97 peak / 0.01 avg reqs/sec
INFO: traffic over all time - 2.97 peak / 0.01 avg reqs/sec
INFO: percentage of throttled transactions to the total number of transactions over past minute - 0.00 %
INFO: percentage of throttled transactions to the total number of transactions over past hour - 0.00 peak / 0.00 avg %
INFO: percentage of throttled transactions to the total number of transactions over past day - 0.00 peak / 0.00 avg %
INFO: percentage of throttled transactions to the total number of transactions over past week - 0.00 peak / 0.00 avg %
INFO: percentage of throttled transactions to the total number of transactions over all time - 0.00 peak / 0.00 avg %
INFO: bandwidth saved over past minute - 0.00 Kb/sec
INFO: bandwidth saved over past hour - 0.00 peak / 0.00 avg Kb/sec
INFO: bandwidth saved over past day - 0.00 peak / 0.00 avg Kb/sec
INFO: bandwidth saved over past week - 0.00 peak / 0.00 avg Kb/sec
INFO: bandwidth saved over all time - 2.01 peak / 0.00 avg Kb/sec
```

How to Read Prox_track.log

- Statistics are snapshots of total number of Packets
Counters are reset after reboot / restart of proxy
- Take statistic from time X and time Y, then compare **change**:

9:01 AM			11:31 AM			
Client Time	1.0 ms	503	Client Time	1.0 ms	516	13
Client Time	1.6 ms	0	Client Time	1.6 ms	0	0
Client Time	2.5 ms	54	Client Time	2.5 ms	56	2
Client Time	4.0 ms	10	Client Time	4.0 ms	10	0
Client Time	6.3 ms	0	Client Time	6.3 ms	0	0
Client Time	10.0 ms	1	Client Time	10.0 ms	1	0
Client Time	15.8 ms	6	Client Time	15.8 ms	6	0
Client Time	25.1 ms	165	Client Time	25.1 ms	165	0
Client Time	39.8 ms	1381	Client Time	39.8 ms	1384	3
Client Time	63.1 ms	1208	Client Time	63.1 ms	1221	13
Client Time	100.0 ms	1224	Client Time	100.0 ms	1280	56
Client Time	158.5 ms	856	Client Time	158.5 ms	900	44
Client Time	251.2 ms	1689	Client Time	251.2 ms	1831	142
Client Time	398.1 ms	227	Client Time	398.1 ms	239	12
Client Time	631.0 ms	99	Client Time	631.0 ms	104	5
Client Time	1000.0 ms	41	Client Time	1000.0 ms	42	1
Client Time	1584.9 ms	37	Client Time	1584.9 ms	38	1
Client Time	2511.9 ms	22	Client Time	2511.9 ms	22	0
Client Time	3981.1 ms	0	Client Time	3981.1 ms	0	0
Client Time	6309.6 ms	42	Client Time	6309.6 ms	42	0

Important Statistics

- Client time:
Total time that the client was waiting until his request was fulfilled
- Hit time:
Time that the WSA is using to fetch content from the cache
- Miss time:
Time that the WSA takes to fetch all Data from the server

```
Client Time      1.0 ms    516
Client Time      1.6 ms     0
Client Time      2.5 ms    56
Client Time      4.0 ms    10
Client Time      6.3 ms     0
Client Time     10.0 ms     1
Client Time     15.8 ms     6
Client Time     25.1 ms    165
Client Time     39.8 ms   1384
Client Time     63.1 ms   1221
Client Time    100.0 ms  1280
Client Time    158.5 ms   900
Client Time    251.2 ms  1831
Client Time    398.1 ms   239
Client Time    631.0 ms   104
Client Time   1000.0 ms    42
Client Time   1584.9 ms    38
Client Time   2511.9 ms    22
Client Time   3981.1 ms     0
Client Time   6309.6 ms    42
```

```
Hit Time         1.0 ms     0
Hit Time         1.6 ms     0
Hit Time         2.5 ms    56
Hit Time         4.0 ms    10
Hit Time         6.3 ms     0
Hit Time        10.0 ms     1
Hit Time        15.8 ms     2
Hit Time        25.1 ms     2
Hit Time        39.8 ms    23
Hit Time        63.1 ms    42
Hit Time       100.0 ms    34
Hit Time       158.5 ms    13
Hit Time       251.2 ms    29
Hit Time       398.1 ms     1
Hit Time       631.0 ms     0
Hit Time      1000.0 ms     2
Hit Time      1584.9 ms     4
Hit Time      2511.9 ms     9
Hit Time      3981.1 ms     0
Hit Time      6309.6 ms     0
```

```
Miss Time        1.0 ms    191
Miss Time        1.6 ms     0
Miss Time        2.5 ms     0
Miss Time        4.0 ms     0
Miss Time        6.3 ms     0
Miss Time       10.0 ms     0
Miss Time       15.8 ms     4
Miss Time       25.1 ms    163
Miss Time       39.8 ms   1361
Miss Time       63.1 ms   1179
Miss Time      100.0 ms  1246
Miss Time      158.5 ms   886
Miss Time      251.2 ms  1802
Miss Time      398.1 ms   238
Miss Time      631.0 ms   104
Miss Time     1000.0 ms    40
Miss Time     1584.9 ms    34
Miss Time     2511.9 ms    13
Miss Time     3981.1 ms     0
Miss Time     6309.6 ms    42
```

Important Statistics (2)

- Server Transaction time:
Time for the total transaction to the Server to be finished.

High Values can mean “upstream” problems (firewall, router, ISP, upstream proxy)

```
Server Transaction Time    1.0 ms    0
Server Transaction Time    1.6 ms    2
Server Transaction Time    2.5 ms    0
Server Transaction Time    4.0 ms    0
Server Transaction Time    6.3 ms    0
Server Transaction Time   10.0 ms    0
Server Transaction Time   15.8 ms   22
Server Transaction Time   25.1 ms   33
Server Transaction Time   39.8 ms  471
Server Transaction Time   63.1 ms  513
Server Transaction Time  100.0 ms 2248
Server Transaction Time  158.5 ms 1054
Server Transaction Time  251.2 ms 1052
Server Transaction Time  398.1 ms 1053
Server Transaction Time  631.0 ms  649
Server Transaction Time 1000.0 ms   97
Server Transaction Time 1584.9 ms   27
Server Transaction Time 2511.9 ms    15
Server Transaction Time 3981.1 ms    10
Server Transaction Time 6309.6 ms   413
```

- Server wait time:
Time until WSA gets the first byte from the Server

```
Server Wait Time          1.0 ms    0
Server Wait Time          1.6 ms    0
Server Wait Time          2.5 ms    0
Server Wait Time          4.0 ms    0
Server Wait Time          6.3 ms    0
Server Wait Time         10.0 ms    0
Server Wait Time         15.8 ms   41
Server Wait Time         25.1 ms 1993
Server Wait Time         39.8 ms 1102
Server Wait Time         63.1 ms  372
Server Wait Time        100.0 ms  846
Server Wait Time        158.5 ms 1211
Server Wait Time        251.2 ms 1143
Server Wait Time        398.1 ms  180
Server Wait Time        631.0 ms   78
Server Wait Time       1000.0 ms   15
Server Wait Time       1584.9 ms    1
Server Wait Time       2511.9 ms    0
Server Wait Time       3981.1 ms    0
Server Wait Time       6309.6 ms   14
```

Important Statistics (3)

- DNS Time:
Time for the WSA to do a DNS Resolution

High time does indicate a problem with the DNS Server

DNS Time	1.0 ms	146
DNS Time	1.6 ms	609
DNS Time	2.5 ms	96
DNS Time	4.0 ms	21
DNS Time	6.3 ms	4
DNS Time	10.0 ms	1
DNS Time	15.8 ms	37
DNS Time	25.1 ms	18
DNS Time	39.8 ms	6
DNS Time	63.1 ms	2
DNS Time	100.0 ms	5
DNS Time	158.5 ms	7
DNS Time	251.2 ms	0
DNS Time	398.1 ms	1
DNS Time	631.0 ms	1
DNS Time	1000.0 ms	1
DNS Time	1584.9 ms	0
DNS Time	2511.9 ms	5
DNS Time	3981.1 ms	0
DNS Time	6309.6 ms	0

Important Statistics (4)

- Auth Helper Wait:
Time to wait for an authentication request until its validated from the AD / LDAP

High time indicates a problem with the connection to the authentication Server

Auth Helper Wait Time	1.0 ms	7
Auth Helper Wait Time	1.6 ms	0
Auth Helper Wait Time	2.5 ms	0
Auth Helper Wait Time	4.0 ms	0
Auth Helper Wait Time	6.3 ms	0
Auth Helper Wait Time	10.0 ms	0
Auth Helper Wait Time	15.8 ms	0
Auth Helper Wait Time	25.1 ms	0
Auth Helper Wait Time	39.8 ms	0
Auth Helper Wait Time	63.1 ms	0
Auth Helper Wait Time	100.0 ms	0
Auth Helper Wait Time	158.5 ms	0
Auth Helper Wait Time	251.2 ms	0
Auth Helper Wait Time	398.1 ms	0
Auth Helper Wait Time	631.0 ms	0
Auth Helper Wait Time	1000.0 ms	0
Auth Helper Wait Time	1584.9 ms	0
Auth Helper Wait Time	2511.9 ms	0
Auth Helper Wait Time	3981.1 ms	0
Auth Helper Wait Time	6309.6 ms	0

- Auth Helper Service:
Time until an authentication request is fully validated

Check if IP address is already authenticated, check surrogates, etc...

Auth Helper Service Time	1.0 ms	3
Auth Helper Service Time	1.6 ms	25
Auth Helper Service Time	2.5 ms	251
Auth Helper Service Time	4.0 ms	285
Auth Helper Service Time	6.3 ms	12
Auth Helper Service Time	10.0 ms	2
Auth Helper Service Time	15.8 ms	3
Auth Helper Service Time	25.1 ms	1
Auth Helper Service Time	39.8 ms	0
Auth Helper Service Time	63.1 ms	0
Auth Helper Service Time	100.0 ms	220
Auth Helper Service Time	158.5 ms	17
Auth Helper Service Time	251.2 ms	9
Auth Helper Service Time	398.1 ms	5
Auth Helper Service Time	631.0 ms	0
Auth Helper Service Time	1000.0 ms	1
Auth Helper Service Time	1584.9 ms	0
Auth Helper Service Time	2511.9 ms	0
Auth Helper Service Time	3981.1 ms	0
Auth Helper Service Time	6309.6 ms	28

Important Statistics (5)

- WBRService Time:
Time for the WSA to check the reputation score
- Webcat Service time:
Time for the WSA to check the URL Category
- AVC Header Scan Service Time:
Time to check the Header of a request against the AVC Signatures
- AVC Body Scan Service time:
Time to check the body of a request against the AVC Signatures

```
WBRService Time      1.0 ms  3963
WBRService Time      1.6 ms  2516
WBRService Time      2.5 ms   324
WBRService Time      4.0 ms    68
WBRService Time      6.3 ms    29
WBRService Time     10.0 ms    16
WBRService Time     15.8 ms    36
WBRService Time     25.1 ms    34
WBRService Time     39.8 ms    13
WBRService Time     63.1 ms     7
WBRService Time    100.0 ms     9
WBRService Time    158.5 ms    11
WBRService Time    251.2 ms     7
WBRService Time    398.1 ms    20
WBRService Time    631.0 ms    60
WBRService Time   1000.0 ms     8
WBRService Time   1584.9 ms    11
WBRService Time   2511.9 ms     4
WBRService Time   3981.1 ms     0
WBRService Time   6309.6 ms    28
```

```
AVC Header Scan Service Time  10.0 ms  14085
AVC Header Scan Service Time  17.3 ms   36
AVC Header Scan Service Time  30.0 ms   23
AVC Header Scan Service Time  52.1 ms   11
AVC Header Scan Service Time  90.3 ms    0
AVC Header Scan Service Time 156.5 ms    1
AVC Header Scan Service Time 271.3 ms    0
AVC Header Scan Service Time 470.3 ms    0
AVC Header Scan Service Time 815.2 ms    0
AVC Header Scan Service Time 1413.1 ms    0
AVC Header Scan Service Time 2449.5 ms    0
AVC Header Scan Service Time 4246.0 ms    0
AVC Header Scan Service Time 7360.2 ms    0
AVC Header Scan Service Time 12758.5 ms    0
AVC Header Scan Service Time 22116.0 ms    0
AVC Header Scan Service Time 38336.6 ms    0
AVC Header Scan Service Time 66454.0 ms    0
AVC Header Scan Service Time 115193.7 ms    0
AVC Header Scan Service Time 199680.7 ms    0
AVC Header Scan Service Time 346133.5 ms    0
```

Important Statistics (6)

- Sophos, McAfee, Webroot
- Service Time:
Time that the Scanner used to scan the object
- Service Queue Time:
Time that the object stayed in the queue

- Adaptive Scanning Service Time:
Time for the adaptive scanning process to scan an object:

```
Sophos Queue Time      10.0 ms 456
Sophos Queue Time      17.3 ms 0
Sophos Queue Time      30.0 ms 0
Sophos Queue Time      52.1 ms 0
Sophos Queue Time      90.3 ms 0
Sophos Queue Time     156.5 ms 0
Sophos Queue Time     271.3 ms 0
Sophos Queue Time     470.3 ms 0
Sophos Queue Time     815.2 ms 0
Sophos Queue Time    1413.1 ms 0
Sophos Queue Time    2449.5 ms 0
Sophos Queue Time    4246.0 ms 0
Sophos Queue Time    7360.2 ms 0
Sophos Queue Time   12758.5 ms 0
Sophos Queue Time   22116.0 ms 0
Sophos Queue Time   38336.6 ms 0
Sophos Queue Time   66454.0 ms 0
Sophos Queue Time  115193.7 ms 0
Sophos Queue Time  199680.7 ms 0
Sophos Queue Time  346133.5 ms 0
```

```
Webroot Queue Time     10.0 ms 4
Webroot Queue Time     17.3 ms 0
Webroot Queue Time     30.0 ms 0
Webroot Queue Time     52.1 ms 0
Webroot Queue Time     90.3 ms 0
Webroot Queue Time    156.5 ms 0
Webroot Queue Time    271.3 ms 0
Webroot Queue Time    470.3 ms 0
Webroot Queue Time    815.2 ms 0
Webroot Queue Time   1413.1 ms 0
Webroot Queue Time   2449.5 ms 0
Webroot Queue Time   4246.0 ms 0
Webroot Queue Time   7360.2 ms 0
Webroot Queue Time   12758.5 ms 0
Webroot Queue Time   22116.0 ms 0
Webroot Queue Time   38336.6 ms 0
Webroot Queue Time   66454.0 ms 0
Webroot Queue Time  115193.7 ms 0
Webroot Queue Time  199680.7 ms 0
Webroot Queue Time  346133.5 ms 530
```

```
Adaptive Scanning Service Time      1.0 ms 415
Adaptive Scanning Service Time      1.6 ms 17
Adaptive Scanning Service Time      2.5 ms 5
Adaptive Scanning Service Time      4.0 ms 7
Adaptive Scanning Service Time      6.3 ms 3
Adaptive Scanning Service Time     10.0 ms 3
Adaptive Scanning Service Time     15.8 ms 2
Adaptive Scanning Service Time     25.1 ms 3
Adaptive Scanning Service Time     39.8 ms 2
Adaptive Scanning Service Time     63.1 ms 2
Adaptive Scanning Service Time    100.0 ms 0
Adaptive Scanning Service Time    158.5 ms 0
Adaptive Scanning Service Time    251.2 ms 0
Adaptive Scanning Service Time    398.1 ms 0
Adaptive Scanning Service Time    631.0 ms 0
Adaptive Scanning Service Time   1000.0 ms 0
Adaptive Scanning Service Time   1584.9 ms 2
Adaptive Scanning Service Time   2511.9 ms 0
Adaptive Scanning Service Time   3981.1 ms 0
Adaptive Scanning Service Time  6309.6 ms 0
```

Cisco *live!*

Adaptive Scanning

- Each type of object gets a RISK Score assigned
- Score is based on Type of object, effectiveness of malware scanner for this type and WBRS (WBRS must be enabled on WSA)
- Appliance will scan objects with the Scanner that is most appropriate for this object type
- If appliance has a performance problem with the Anti Malware Scanners, it will drop objects not to be scanned

Example: Don't scan *.jpg files with McAfee when they are coming from Websites with a good reputation.

Adaptive Scanning Drop Distribution

Risk Score	McAfee	Sophos	Webroot
0	0/0 (0.00% dropped)	0/0 (0.00% dropped)	0/454 (0.00% dropped)
1	0/240 (0.00% dropped)	0/50 (0.00% dropped)	0/0 (0.00% dropped)
2	0/7 (0.00% dropped)	0/208 (0.00% dropped)	0/0 (0.00% dropped)
3	0/68 (0.00% dropped)	0/89 (0.00% dropped)	0/0 (0.00% dropped)
4	0/0 (0.00% dropped)	0/52 (0.00% dropped)	0/0 (0.00% dropped)
5	0/40 (0.00% dropped)	0/0 (0.00% dropped)	0/0 (0.00% dropped)
6	0/37 (0.00% dropped)	0/8 (0.00% dropped)	0/0 (0.00% dropped)
7	0/45 (0.00% dropped)	0/14 (0.00% dropped)	0/0 (0.00% dropped)
8	0/2 (0.00% dropped)	0/16 (0.00% dropped)	0/2 (0.00% dropped)
9	0/19 (0.00% dropped)	0/19 (0.00% dropped)	0/2 (0.00% dropped)
10	0/0 (0.00% dropped)	0/2 (0.00% dropped)	0/0 (0.00% dropped)

Customising the Access Log

	<input type="radio"/> Squid Details
Custom Fields (optional):	<input type="text" value="%m AUTH: %>a DNS: %>d R"/>
File Name:	<input type="text" value="aclog"/>

Add custom field like:
“%m” (=Authentication Method)
to the access_log

- Variables can be appended in the Access Logs
- Variables are to be found in the ONLINE HELP UI, some older Versions of WSA Software might not have the full list

Customising the Access Log - Example

%m AUTH: %:>a DNS: %:>d REP: %:>r

Any Text acting as a comment for readability

%m : Authentication Method
%:>a : Authentication Wait time
%:>d : DNS Wait time
%:>r : Reputation Wait time

```
1351782495.550 428 172.16.16.10 TCP_MISS/302 760 GET http://www.oktoberfest.de/ "MUNLAB-IP1\administrator@munlabipcom"
DEFAULT_PARENT/64.103.36.133 text/html DEFAULT_CASE_12-MunlabIP_Policy-ID.MunlabIP-DefaultGroup-NONE-NONE-DefaultGroup
<IW_alc,4.9,0,"",0,0,0,0,"-",-1,0,-1,"",0,0,"-","-","-",IW_alc,-,"Unknown",-,"Unknown","Unknown",-,"-",14.21,0,Lo
cal,"Unknown","> - NTLMSSP AUTH: 0 DNS: 132 REP: 13
1351782495.827 274 172.16.16.10 TCP_MISS/200 42101 GET http://www.oktoberfest.de/de "MUNLAB-IP1\administrator@munlabipc
om" DEFAULT_PARENT/64.103.36.133 text/html DEFAULT_CASE_12-MunlabIP_Policy-ID.MunlabIP-DefaultGroup-NONE-NONE-DefaultG r
oup <IW_alc,4.9,0,"-","",0,0,0,0,"-",-1,0,-1,"",0,0,"-","-","-",IW_alc,-,"Unknown",-,"Unknown","Unknown",-,"-",1229.2
3,0,Local,"Unknown","> - NTLMSSP AUTH: 0 DNS: 0 REP: 1
1351782496.123 94 172.16.16.10 TCP_MISS/200 2556 GET http://www.oktoberfest.de/css/of/basemod_2col_left_31.css?v=201206
28 "MUNLAB-IP1\administrator@munlabipcom" DEFAULT_PARENT/64.103.36.133 text/css DEFAULT_CASE_12-MunlabIP_Policy-ID.Mun l
abIP-DefaultGroup-NONE-NONE-DefaultGroup <IW_alc,4.9,0,"-","",0,0,0,0,"-",-1,0,-1,"",0,0,"-","-","-",IW_alc,-,"Unknown",
-,"Unknown","Unknown",-,"-",217.53,0,Local,"Unknown","> - NTLMSSP AUTH: 0 DNS: 0 REP: 1
1351782496.309 96 172.16.16.10 TCP_MISS/200 8346 GET http://www.oktoberfest.de/css/yaml/core/base.css "MUNLAB-IP1\admin
```

Customising the Access Log – Example(2)

Destination IP %k

Extremely useful in Dual-Stack Environments to find out whether WSA makes the outgoing connection on IPv4 or IPv6!

```
1389363752.919 16 2001:420:44e6:2013::30 TCP_MISS/304 328 GET http://www.ripe.net/pb_cl
ID.MUNSEC-NONE-NONE-NONE-DefaultGroup <IW_comp,4.9,0,"-",0,0,0,-,"-",,-,-,-,"-",,-,-,-,"-",
193.0.6.139 NTLMSSP AUTH: 0 DNS: 0 REP: 1 SEBR: 3 CFBWR: 0
```

Destination IP = v4

Source IP from Client = IPv6

Using SPLUNK to Extract Data

Definition of Regex to look for the Keywords we defined for the Accesslog customisation

Search

```
host="munlab-wsa01" |rex field=_raw "DNS:\s(?:<trackdns>\d+)\sREP:\s(?:<trackrep>\d+)" |chart avg(trackrep),avg(trackdns) by dest_domain
```

55 results from 3:00:00 PM February 11 to 3:38:05 PM February 12, 2013

    Export  Options

Overlay:

	dest_domain ↕	avg(trackrep) ↕	avg(trackdns) ↕
1	2o7.net	526.000000	8.500000
2	7x24web.net	0.000000	0.000000
3	212.27.60.27	150.530303	0.000000
4	aachen.de	0.000000	0.000000
5	adform.net	27.000000	26.666667
6	ate.info	0.000000	0.000000
7	atosworldline.com	0.000000	0.000000
8	bayern.de	1669.000000	197.000000
9	bild.iwbox.de	2.000000	1.000000
10	bilder.bild.de	1.468085	0.042553

Cisco *live!*

Using SPLUNK to Extract Data (2)

Extraction of the values to be done permanently in SPLUNK

Field extractions

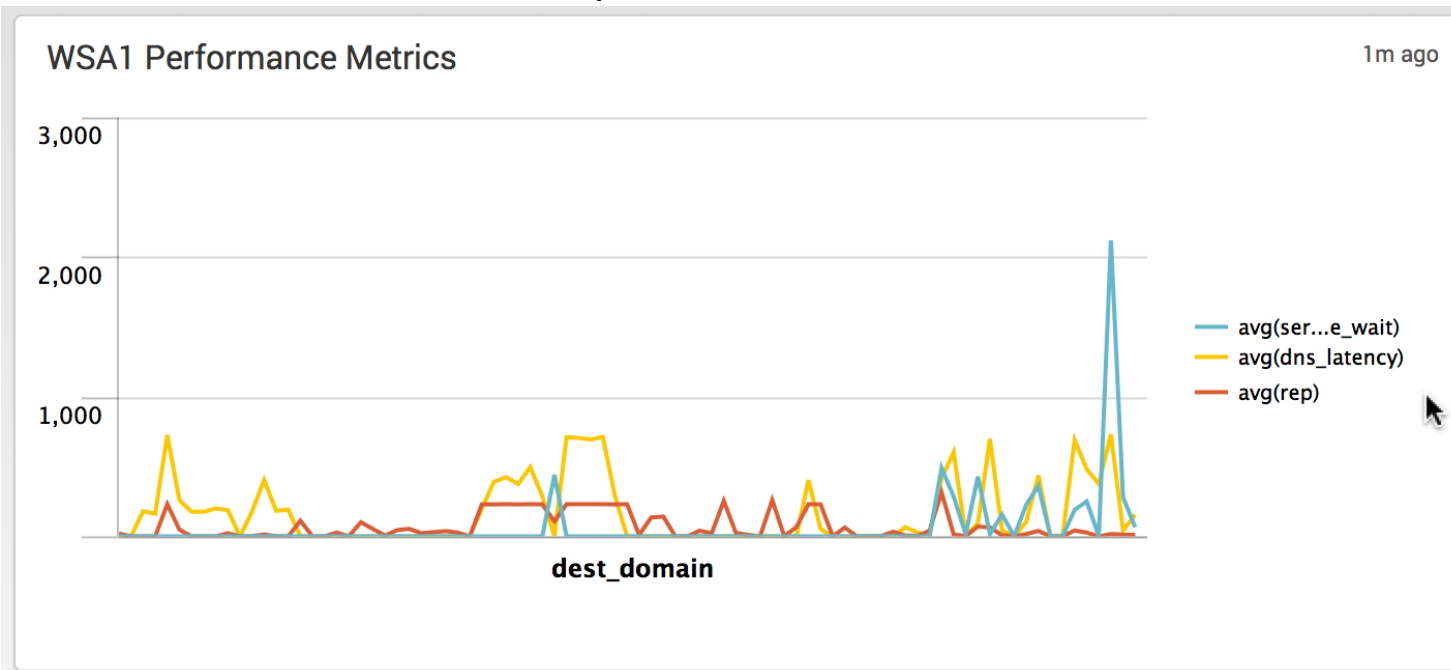
New

Showing 1-7 of 7 items

Name ↕		Extraction/Transform ↕
splunk_web_service : EXTRACT-useragent	Inline	userAgent=(?P<browser>[^\s]+)
splunkd : EXTRACT-fields	Inline	(?i)^(?:[^\s]*){2}(?:[^\s-]+)+)?(?P<log_level>[^\s]*)\s+(?P<component>[^\s]+) - (?P<message>.+)
wsa_accesslogs : EXTRACT-Auth_type	Inline	>\s+\s+\s+(?P<Auth_type>\w+)
wsa_accesslogs : EXTRACT-auth_wait_time	Inline	AUTH:.(?P<auth_wait_time>\d+)
wsa_accesslogs : EXTRACT-dns_latency	Inline	DNS:.(?P<dns_latency>\d+)
wsa_accesslogs : EXTRACT-rep	Inline	REP:.(?P<rep>\d+)
wsa_accesslogs : EXTRACT-server_first_byte_wait	Inline	SFBR:.(?P<server_first_byte_wait>\d+)

Using SPLUNK to Extract Data(3)

- SPLUNK Report on the Average time for REPUTATION, DNS Resolution and SERVER_FIRST_BYTE_WAIT per Domain

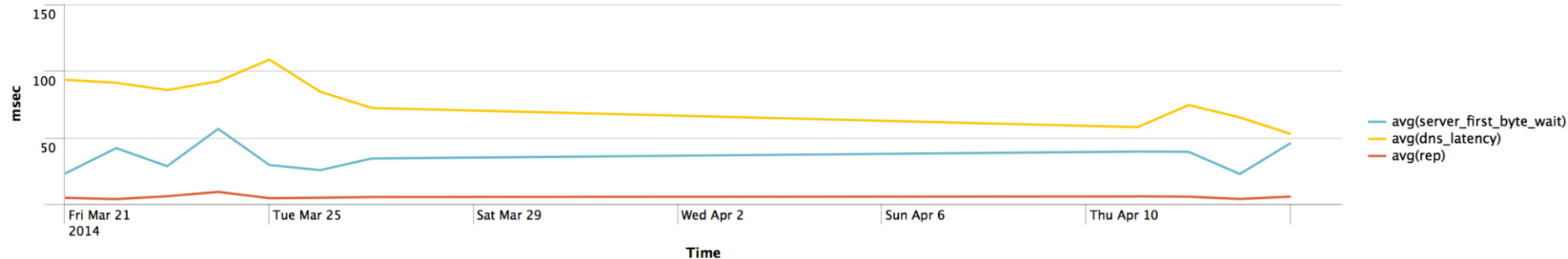


Using SPLUNK to Extract Data(4)

- SPLUNK Report on the Average time for REPUTATION, DNS Resolution and SERVER_FIRST_BYTE_WAIT for the last 30 days

WSA1 TIMECHART 30 DAYS PERFORMANCE

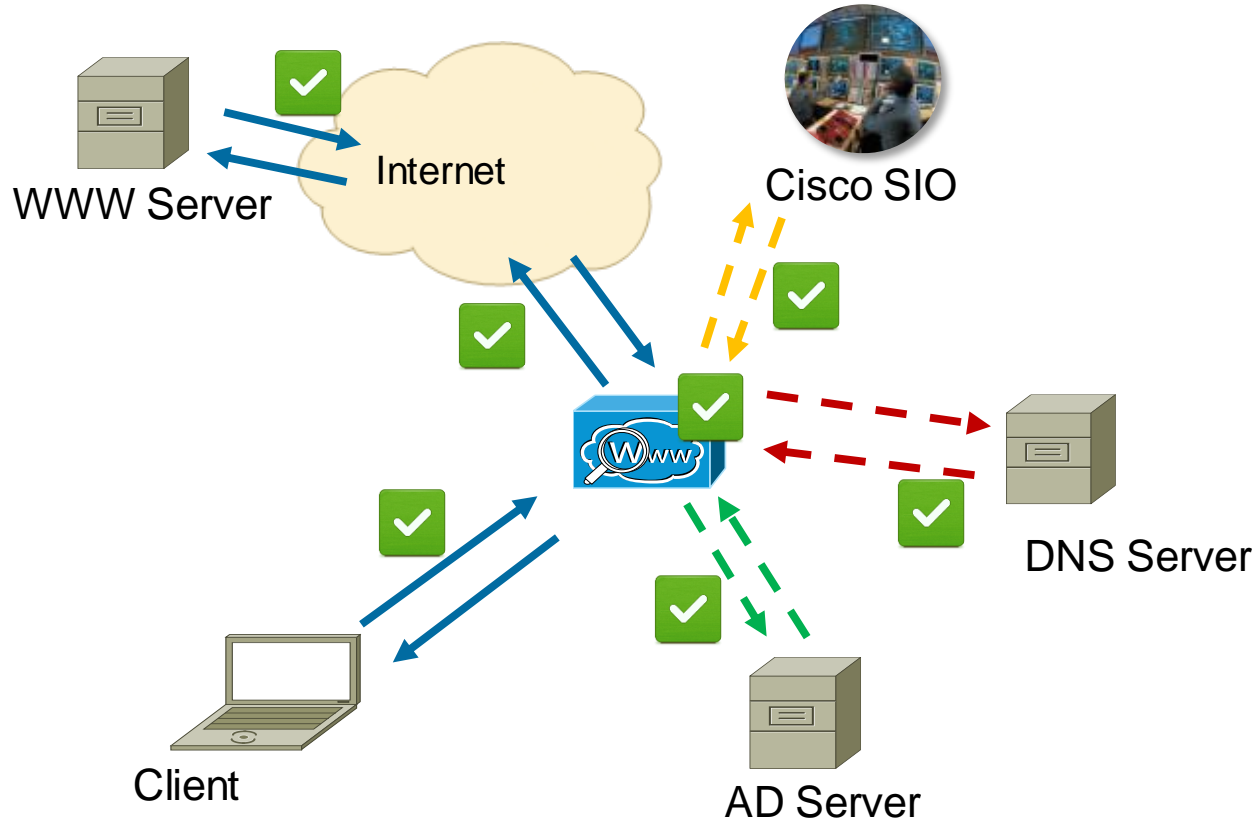
4m ago



Summary for WSA Performance Analysis

- WSA has very detailed logs to troubleshoot performance issues
- Use prox_stat.log file for general performance checks
- Use customising the Access Logs for detailed checking of single requests
- SPLUNK is a great tool to help you analyse especially when combined with customised logs!

WSA Performance Analysis



Conclusion

- Explicit and Transparent mode both support Deployment using IPv6 & IPv4
- Kerberos Authentication can provide Single-Sign-On for windows and non-windows clients
- AMP on WSA is an additional Scanner for Malware, especially targeted against APTs
- WSA provides great details for troubleshooting performance problems through custom variables
- Easy visualisation of critical conditions with customised logging and 3rd Party tools like SPLUNK



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco *live!*



Thank you.

Cisco *live!*



CISCO