# Nyt fra Email- og Websecurity

# Web Security Appliance

Mikael Grotrian, CISSP, CISM, CCSK, GISF, ITIL, PRINCE2, TOGAF Certified
Consulting Systems Engineer, Cyber Security, Denmark

# Archive Inspection

10.1

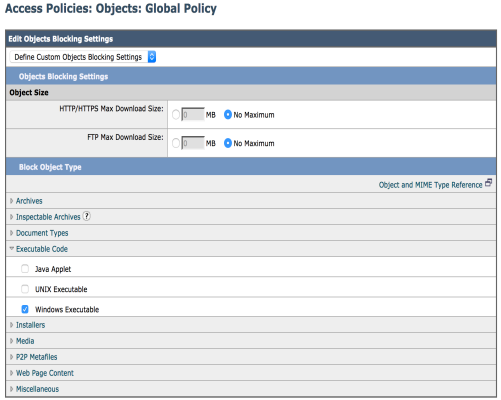
## Archive File

WSA

**“abc.rar”**

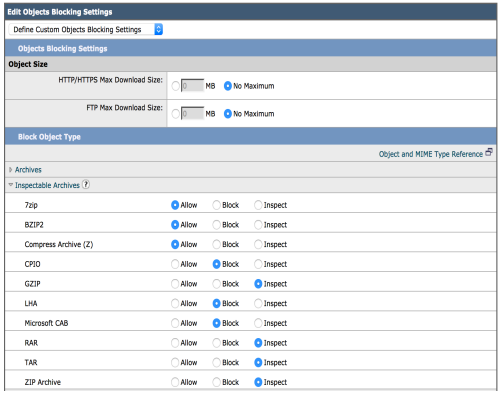
- ✓ 1.exe
- ✓ 2.exe
- ✓ 3.exe
- ✓ 4.doc

Access Policies > Objects > Executable Code




As per the IT Policies ”EXE” files are blocked.

Access Policies > Objects >Inspectable Archives




We support **10** different format Inspect Archive files types.

**“abc.rar”** is blocked as it contains **“EXE”** File

© 2015 Cisco and/or its affiliates. All rights reserved

10.1

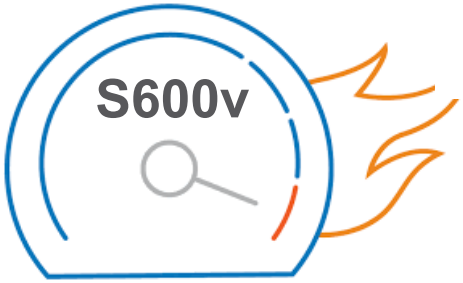
# New Web Security Virtual Platform

## Increased Performance

CPU's
12 Cores

Memory
24 GB RAM

Disk Space
2.4 TB




Large Enterprise

vmware

KVM

**2 X S300v** = 2X MORE POWERFUL **S600v** = **S670 or S390**

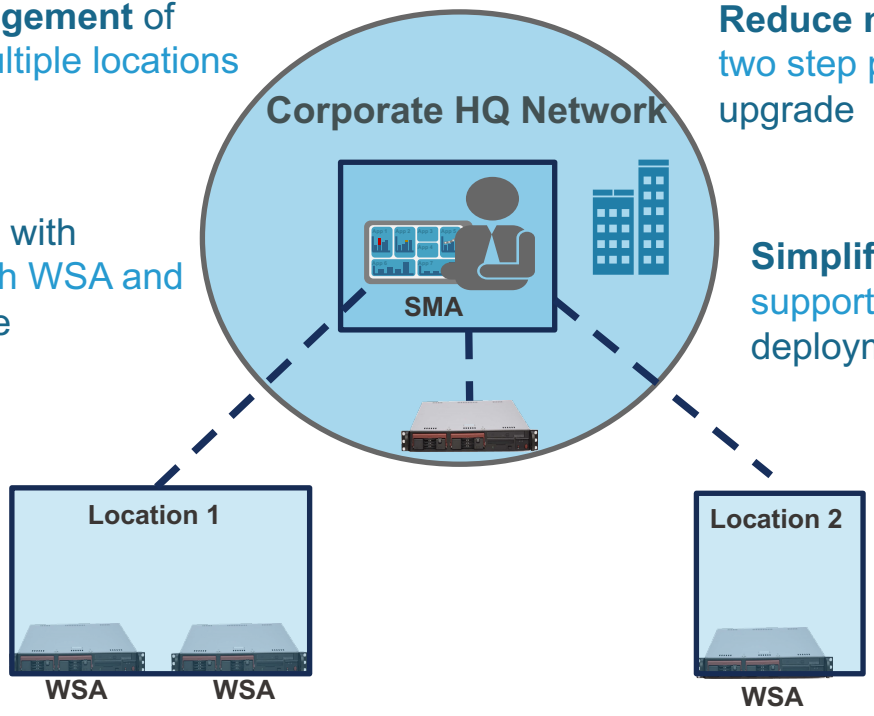
© 2015 Cisco and/or its affiliates. All rights reserved

# Centralized Upgrade

10.1

**Central software management** of multiple WSA across multiple locations

**Flexibility in operations** with capability to choose which WSA and when operation should be performed




**Reduce network downtime** by have two step process of download and upgrade

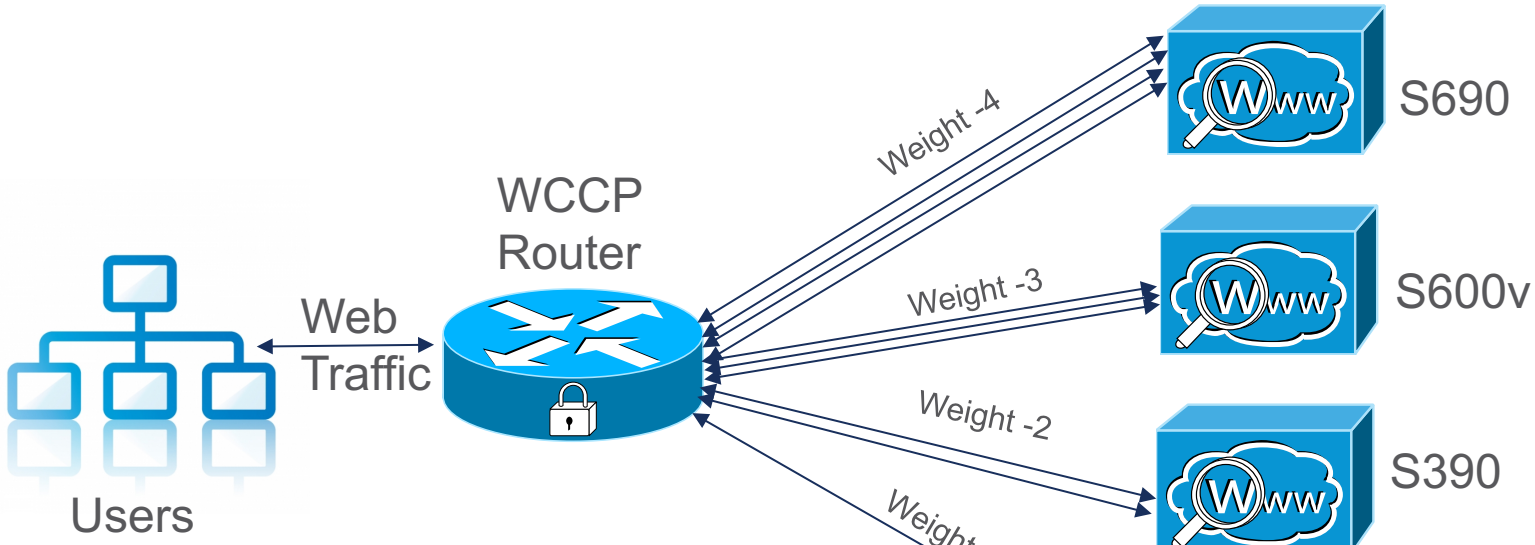
**Simplify global operation** as supported in both physical and virtual deployment models



2015 Cisco and/or its affiliates. All rights reserved

# WCCP Weighted Load Balancing

10.5




The designated WSA should first calculate the total = **4+3+2+1 = 10**

**In case Hash bucket algorithm is being used to balance load:**
**S690** should get **4/10th** of the available hash buckets - **(4/10) X 255**
**S600v** should get **3/10th** of the available hash buckets - **(3/10) X 255**
**S390** should get **2/10th** of the available hash buckets - **(2/10) X 255**
**S190** should get **1/10th** of the available hash buckets - **(1/10) X 255**

© 2015 Cisco and/or its affiliates. All rights reserved

# Industry Recognized Certifications

10.5

WSA AVAILABLE FOR FEDERAL CUSTOMER

FIPS Certification

Common Criteria

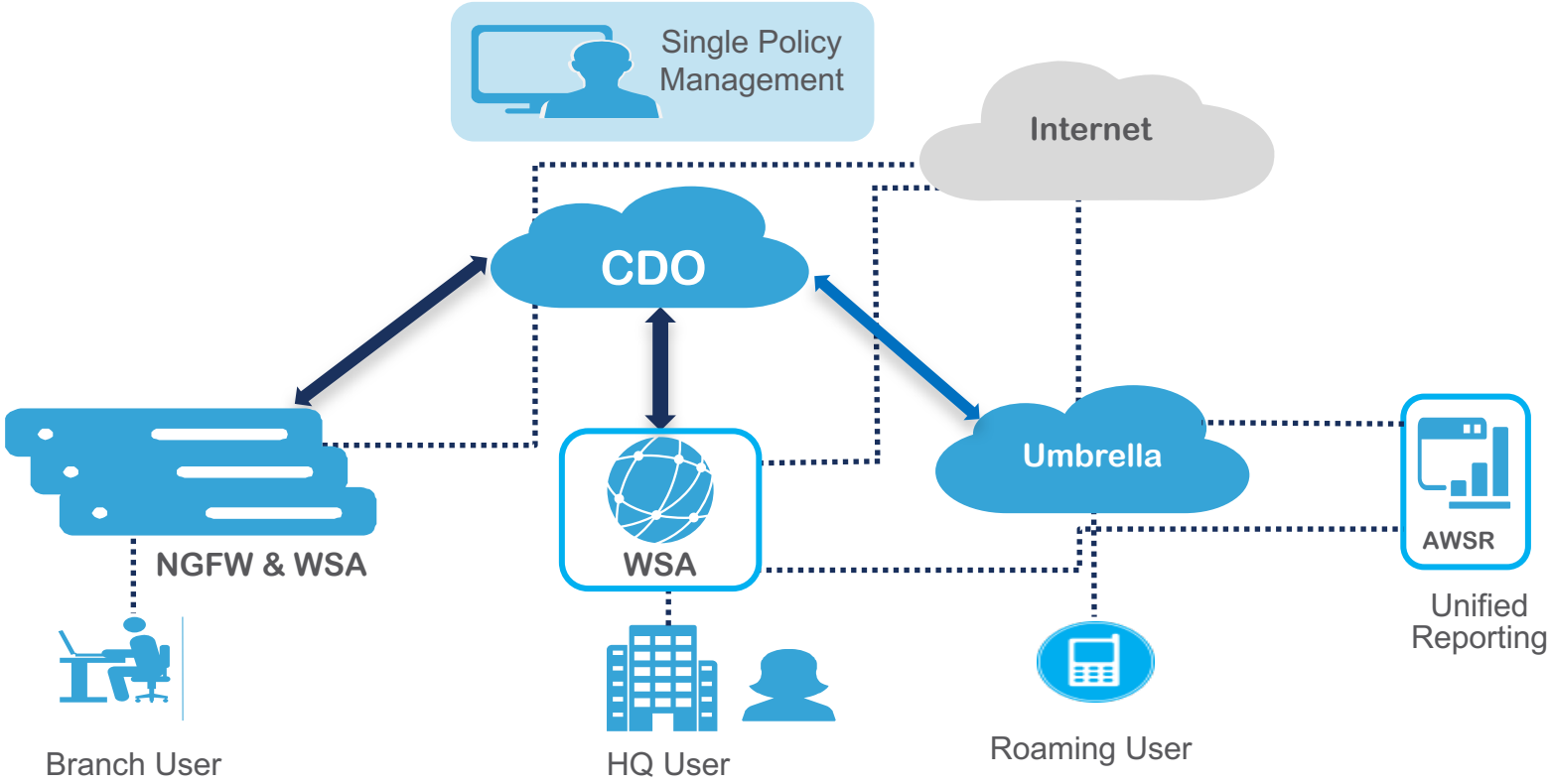
UC - APL

WSA AVAILABLE FOR FEDERAL CUSTOMER

© 2015 Cisco and/or its affiliates. All rights reserved

# CDO Integration

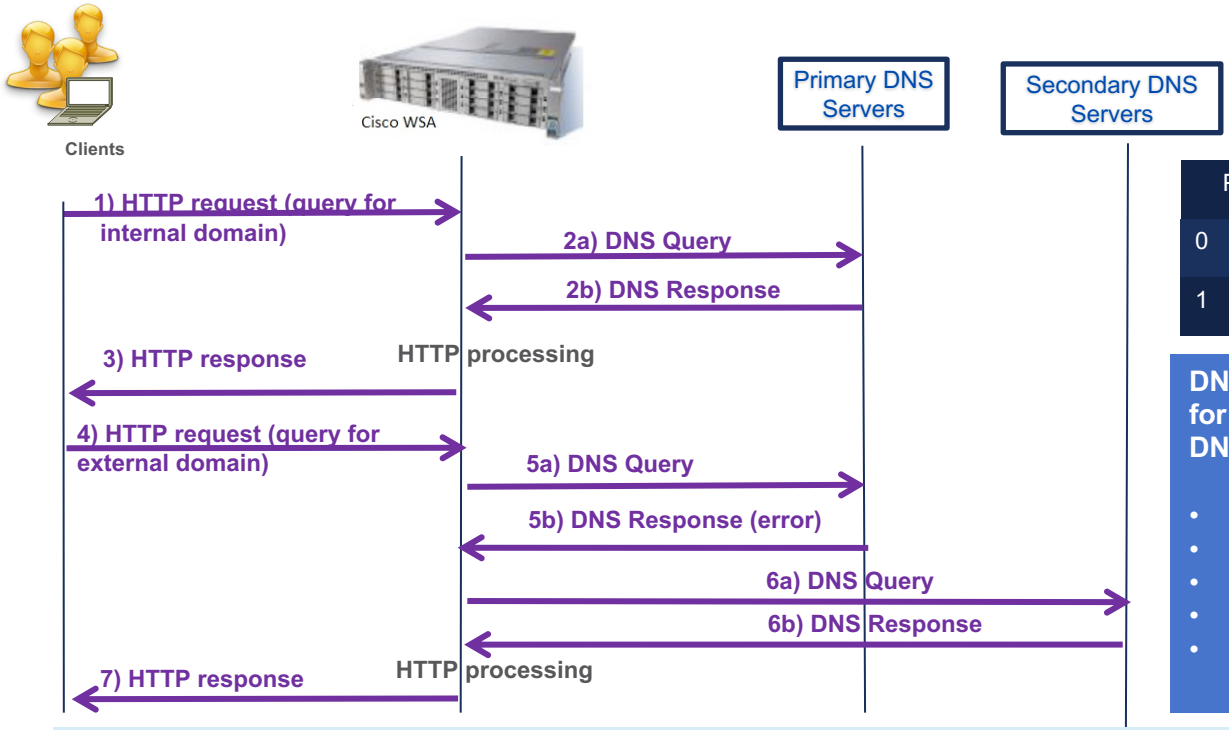
11.0




© 2015 Cisco and/or its affiliates. All rights reserved

# Secondary DNS Servers

11.0




| Primary DNS Server List | | Secondary DNS Server List | |
|---|---|---|---|
| 0 | Internal DNS Server 1 | 0 | External DNS Server 1 |
| 1 | Internal DNS Server 2 | 1 | External DNS Server 2 |

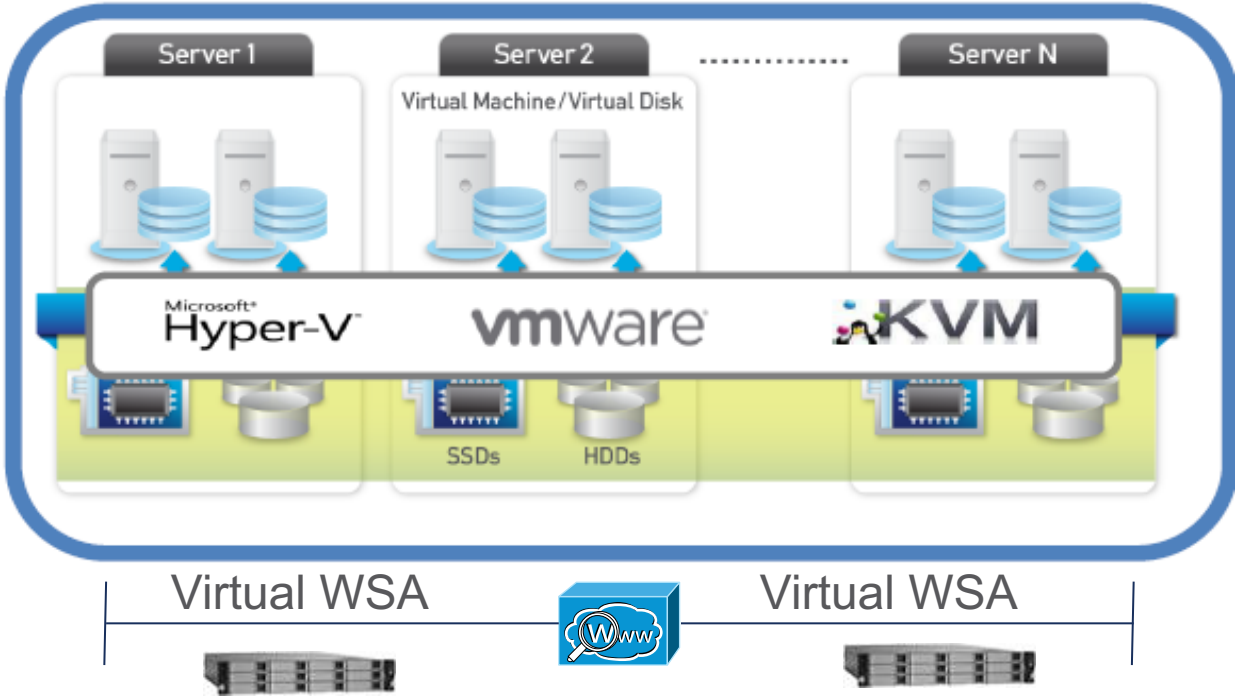
**DNS Response codes from Primary DNS servers for which the DNS query is send to the Secondary DNS Servers:**

- **0, No Error, No Answer Section**
- **2, Server Failure with No Answer section**
- **3, Name Error with No Answer section**
- **4, Not Implemented with No Answer section**
- **5, Refused with No Answer Section**

- Enhanced DNS feature introduces Secondary DNS Table
- By utilizing Primary and Secondary tables of DNS servers for the internal and the external domains, Enhanced DNS feature enables customer to group DNS servers into two lists mainly based on type of records that a particular group of server handles. E.g. internal DNS server group and external DNS server group

11.0

# Hyper V Support

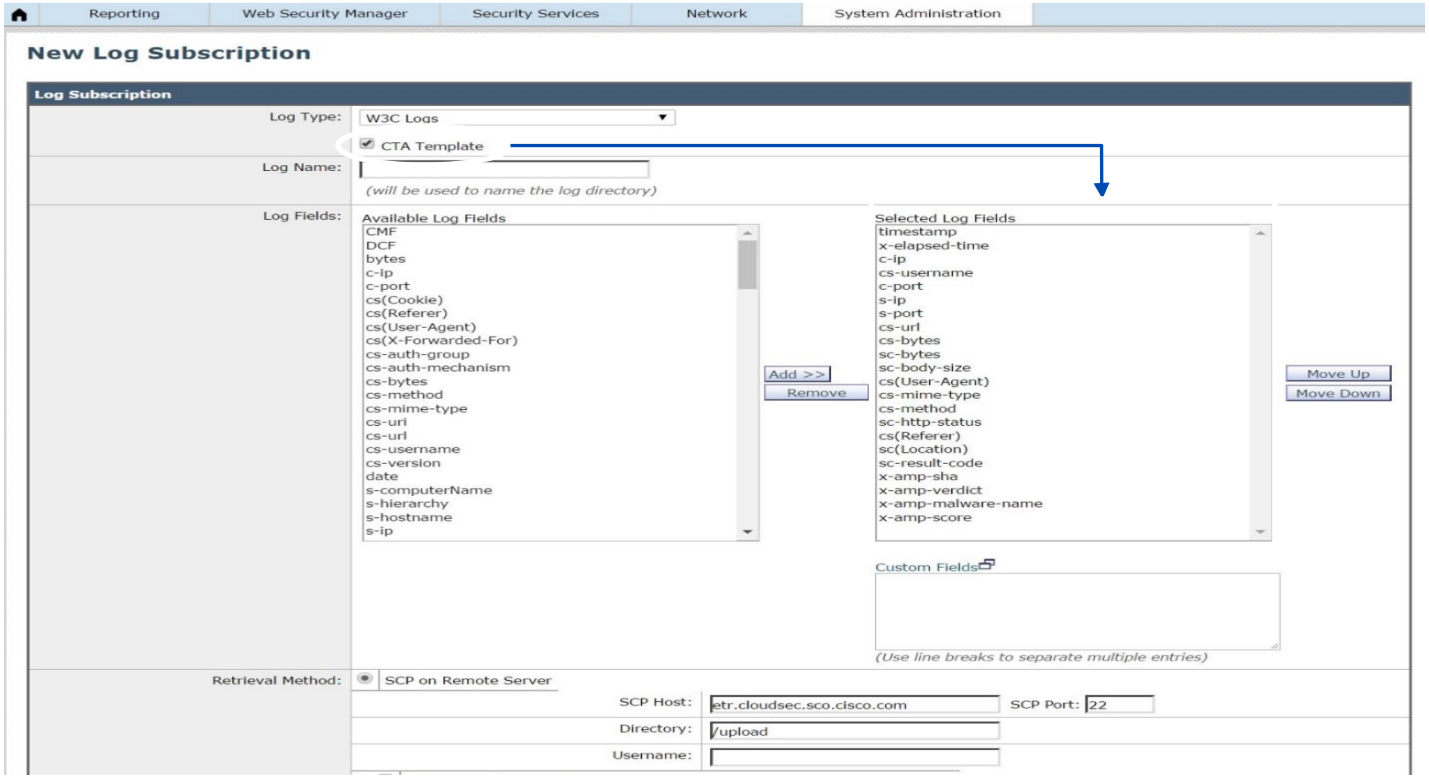



| Virtual WSA Models | Supported |
|---|---|
| S600v | ✓ |
| S300v | ✓ |
| S100v | ✓ |
| S000v (Demo) | ✓ |

© 2015 Cisco and/or its affiliates. All rights reserved

# CTA Template Support

11.0




© 2015 Cisco and/or its affiliates. All rights reserved

# Email Security Appliance

Mikael Grotrian, CISSP, CISM, CCSK, GISF, ITIL, PRINCE2, TOGAF Certified
Consulting Systems Engineer, Cyber Security, Denmark

# Sophos CXMail

SOPHOS

10.0.1

Sophos CXMail is an engine component that extends detection capabilities and uses aggressive context-specific heuristics.

Purposefully designed to stop email distributed threats such as ransomware, it applies stricter rules aimed at active content in email attachments and identifies polymorphic malicious documents and executables.

© 2015 Cisco and/or its affiliates. All rights reserved.

10.0.1

# Macro Detection Content Filter

Macro enabled document detection allows the Email Administrator set Content Filter policies around email attachments containing macros and take the actions of:

- Quarantine the message
- Strip the attachment
- Strip the attachment and add notification text to the message body
- Modify the subject
- Add header
- Forward to another address

© 2015 Cisco and/or its affiliates. All rights reserved.

10.0.1

# Macro Detection Content Filter

Macro Detection Content Filter reporting:

- Number of emails matching the CF
- Top incoming CF matches
- Top outgoing CF matches
- Top file types with macro
- Matches over time
- Matches by internal users

Message Tracking addition to allow searching for emails matching the Macro Detection Content Filter

© 2015 Cisco and/or its affiliates. All rights reserved.

10.0.1

# KVM Support

Being Open Source, KVM is the hypervisor of choice for your price conscious customers and Service Providers, and this release brings KVM to the ESA.

- Can run ESA, WSA, and SMA as virtual machines on a single, more cost effective server
- Neatly fits into the Cisco Security as a Service framework.

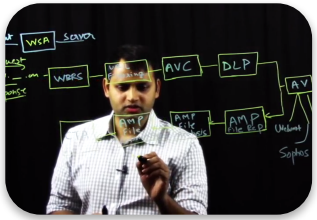
Similar to VMware, configure the machines for the correct amount of RAM, CPU cores, and disk space or you'll throw error messages on the CLI interface.

© 2015 Cisco and/or its affiliates. All rights reserved.

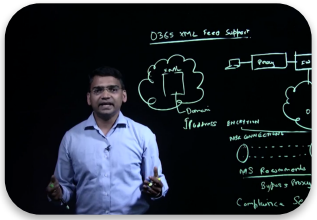
CISCO
TOMORROW starts here.

# Chalk Talk Videos

[WSA Sizing Guide]




[WSA Defense in Depth]




[Office 365 Integration]

[DLP Solution]

[WSA 10.1]

Employee Communities

© 2015 Cisco and/or its affiliates. All rights reserved