



## Leveraging SSL Certificates in the SMP Environment

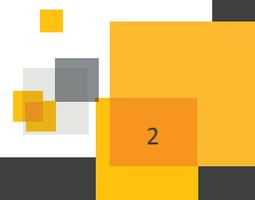
**Tomas Chinchilla**, Sr. Regional Product Manager, Endpoint Management

**Brian Sheedy**, Sr. Principal TEC, Endpoint Management



# Agenda

|   |                                                        |
|---|--------------------------------------------------------|
| 1 | Preparing for HTTPS Communications                     |
| 2 | Implementing HTTPS in the SMP 7.6 Environment          |
| 3 | New Features in SMP 7.6 Infrastructure & Core Settings |
| 4 | Introduction to Cloud-Enabled Management               |

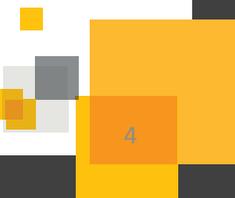




# Preparing for HTTPS Communications

# Why use HTTPS communication in SMP?

- **Accessing the Symantec Management Platform using HTTPS provides these advantages:**
  - Increased security and reliable communication
  - HTTP is unsecured and is vulnerable to man-in-the-middle and eavesdropping attacks.
  - HTTPS is designed to withstand such attacks, and creates a secured channel
- **The following components in your SMP environment can be set to use HTTPS:**
  - Notification Server
  - Site servers (package server, task server, and so on)
  - Symantec Management Agent
  - Client computers
- **You can set up your SMP environment on HTTPS**
  - During SMP installation
  - After the SMP installation is completed using HTTP



## Certificates in SMP 7.6+

- The SMP 7.6 environment supports the following Certificates
  - Self-signed
  - Commercial
  - PKI Infrastructure
- No Magic Bullet or One size fits all...
  - Many combinations exist on our customer environments
- Know when to choose the right one for your design
- Routable vs No-Routable Domains... Which one are you?
  - i.e., Domain = *corp.company.com* or *corp.company.local*
- Certificates must match the FQDN of the Server or Host that the Agent is looking for

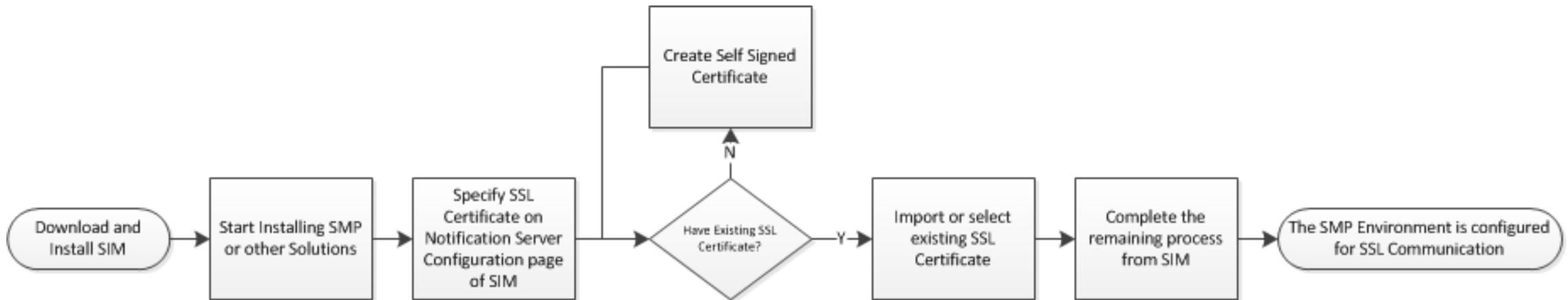




# Implementing HTTPS in the SMP 7.6 Environment

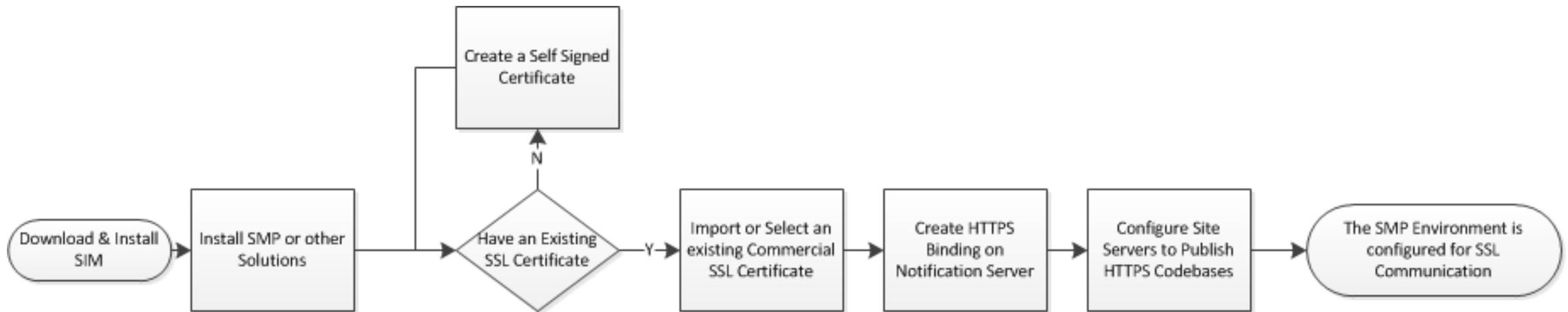
# Implementing SSL During a New SMP Installation

- **Notification Server is automatically configured to use HTTPS:**
  - If You select the **Require HTTPS** on the NS Configuration page in SIM during the installation of the SMP
  - When you roll out Symantec Management Agents from a Notification Server that uses HTTPS
- **Therefore, when you configure HTTPS during SMP installation:**
  - You do not need to configure the SMP components to use HTTPS (NS, SS, Agents...)
  - The Symantec Management Agents are automatically configured to use HTTPS.



# How to configure HTTPS *After* an SMP Installation is Completed

- **When you have not configured HTTPS during an SMP installation:**
  - You can configure the SMP components to use HTTPS after the installation is completed.
- **You must configure the SMP components to use HTTPS**
  - Notification Server, Site Servers, Symantec Management Agent, and the client computers



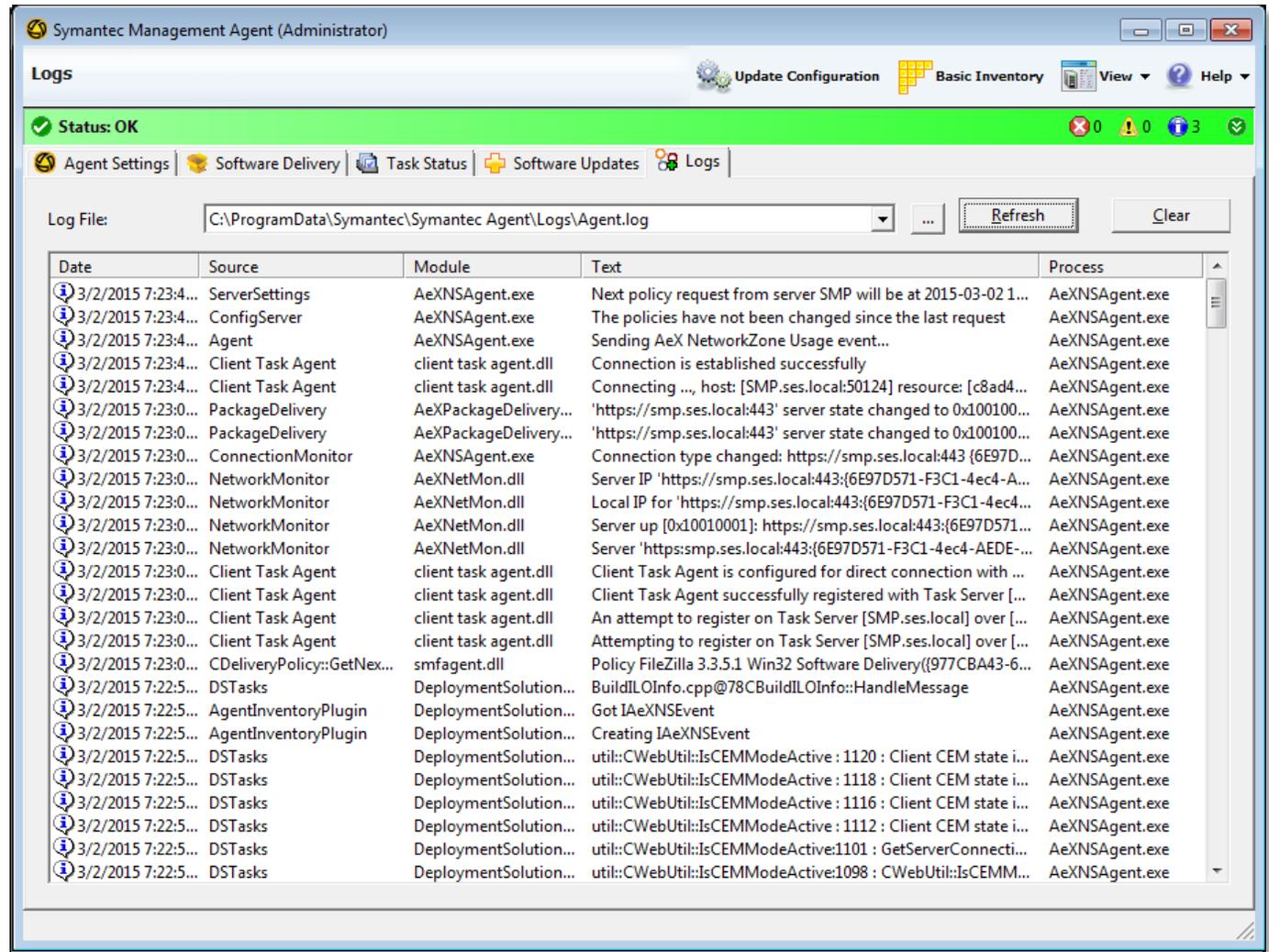


# New Features in SMP 7.6 Infrastructure & Core Settings

# Redesigned Symantec Management Agent User Interface

Symantec Management Agent windows are now combined into one

- **Improvements:**
  - **Usability** - overall user experience is much more convenient
  - **Alerts** - gives a clear understanding about current status of the SMA
  - **Performance** – no lag during tab switching
  - **Logging** - more reliable and accurate logging



# Communication Profiles for the Symantec Management Agent

The image shows a screenshot of the Symantec Management Agent Communication Profiles configuration window. The window title is "Symantec Agent Communication profiles". The interface includes a search bar, a tree view on the left with folders like "UNIX/Linux/Mac", "Windows", "Discovery and Inventory", and "Monitoring and Alerting", and a main configuration area. Several callout boxes are overlaid on the screenshot, providing key information about the profiles:

- Communication Profiles Can be exported/imported to any Notification Server**
- HTTP/HTTPS URL Host Information**
- SSL Certificates**
- Agent Connectivity Credential (ACC)**
- Can also be used for server switching in the Targeted Agent Policy**
- CoM Information Policies Referenced**
- Push/Pull Associations**
- Defines information Agents to establish Notification**
- Can be specified within the push/pull Agent install process**

# Use Cases for Communication Profiles

- **CEM agent off-box upgrade and Disaster Recovery:**
  - Possible to perform off-box upgrade or Disaster Recovery for CEM agents (7.6+)
  - Endpoints do not lose connection permanently and do not need to be recovered with a CEM package re-install
- **Agent registration on the Notification Server:**
  - Allows additional security to credentials transmission
- **HTTPS certificate distribution usability:**
  - Eliminates the need to specify HTTPs connection string and an SSL certificate to be placed on the endpoint during a push installation or during client policy processing when an “alternate URL” was specified.
- **Requirement to specify proxy configuration for the agent:**
  - No need to have the administrator to define proxy server to be used by NS agents to access the NS.
  - No longer uses IE Proxy Settings automatically
- **Improved Connection security:**
  - Eliminates the need for the administrator to define SSL connection security parameters to be used by the Agent during connection to NS.

# Support for HTTP and HTTPS Codebases on Same Package Server

- Package Service now supports providing both HTTP and HTTPS codebases at the same time!
- The webserver codebase configuration options that were formerly radio buttons are now checkboxes.
- Provides package downloads to both Internal and External agents that can be configured to use either HTTP or HTTPS for download

Site Management ▾ Site Server Settings ▾ Package Service ▾ Package Service Settings ▾

## Package Service Settings

View and edit global package service settings.

### Global Package Service Settings

#### Package File Settings

- Delete package files if they are unused for
- Remove automatic site assignments if they are unused for

#### Package Storage Settings

- Allow usage of all the fixed drives when the default storage location runs out of disk space
  - Exclude the system drive

#### Published Codebase Types

- Publish UNC codebase
- Publish IIS hosted codebases (provided IIS is installed)
  - Publish HTTP codebase
  - Publish HTTPS codebase (provided an SSL certificate is installed)

# Redesigned Push/Pull Agent Installation & Settings Page

- Ability to select Communication profile for Push to endpoints
- No longer using ActiveX Controls

The screenshot displays the Symantec Management Console interface for configuring agent installation. The main window, titled "Agent Install", shows the "Symantec Management Agent Installation" section with the profile set to "SMP". Below this is a "Rollout Agent to Computers" section with a table of target computers:

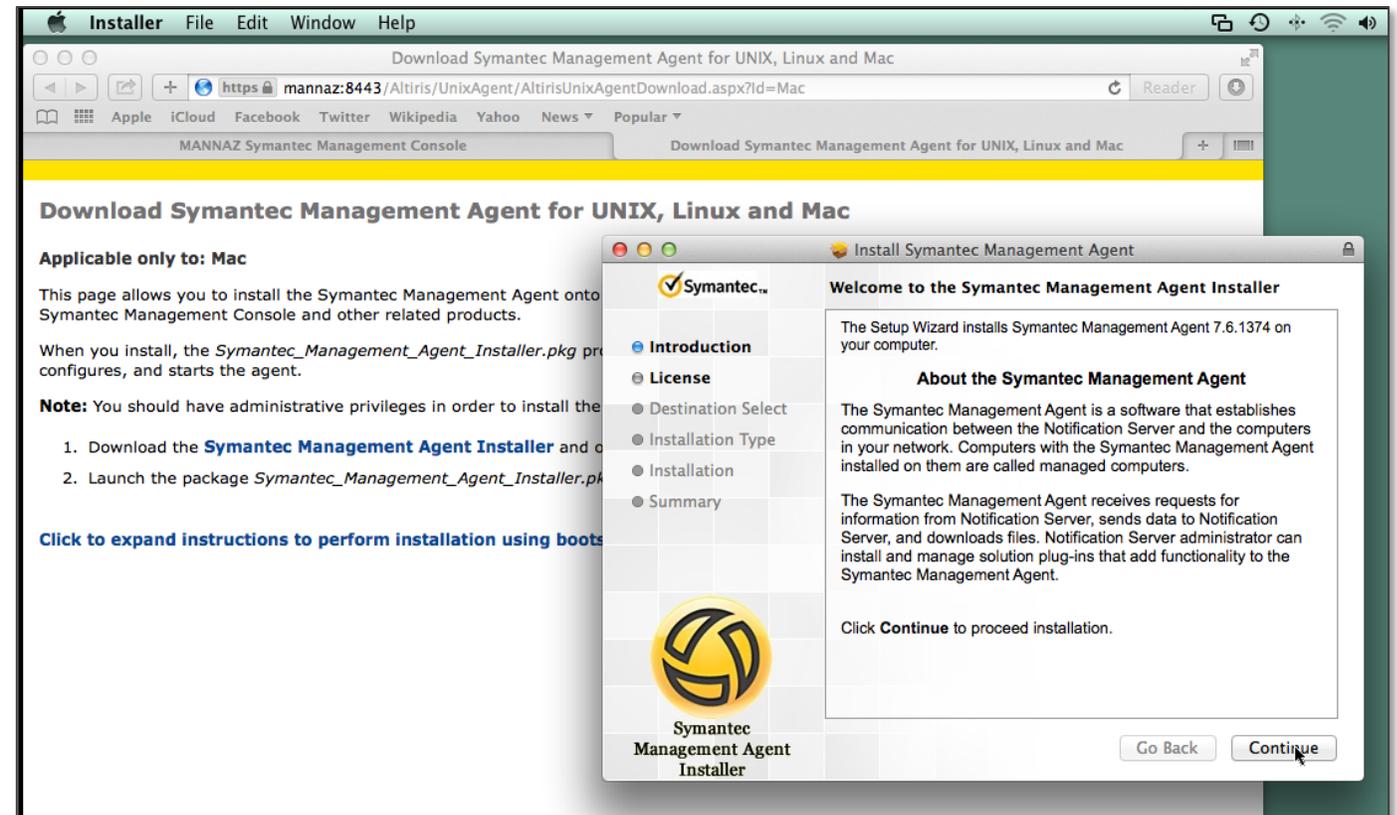
| Name | Domain | OS Name                           |
|------|--------|-----------------------------------|
| DC   | SES    | Windows Server 2008 R2 Enterprise |
| SD7  | SES    | Windows Server 2008 R2 Enterprise |

The "When to Schedule" section is set to "Shared schedule" with "Daily" selected. A secondary dialog box, "Symantec Management Agent Settings", is overlaid on the right, showing "Agent Install Settings" with the profile "SMP" and "Server URL: https://smp:443/Altiris/". It also includes fields for "Override the default installation path" and "Additional parameters", and checkboxes for "Display Symantec Management Agent in the:" (Start menu, System tray, Add/Remove Programs list).

Two red arrows highlight the "Profile: SMP" field in the main window and the "Profile to be used for agent installation:" field in the dialog box.

# Redesigned pull-install for Mac Agent

- Agent package is available for download via browser
- Generation of archive with installation files and configuration on server side
- Implemented native PKG launcher for Agent installation
- Mac packages officially signed
- Standard Mac Installer UI is used for package rollout
- Command line installation using aex-bootstrap is still supported

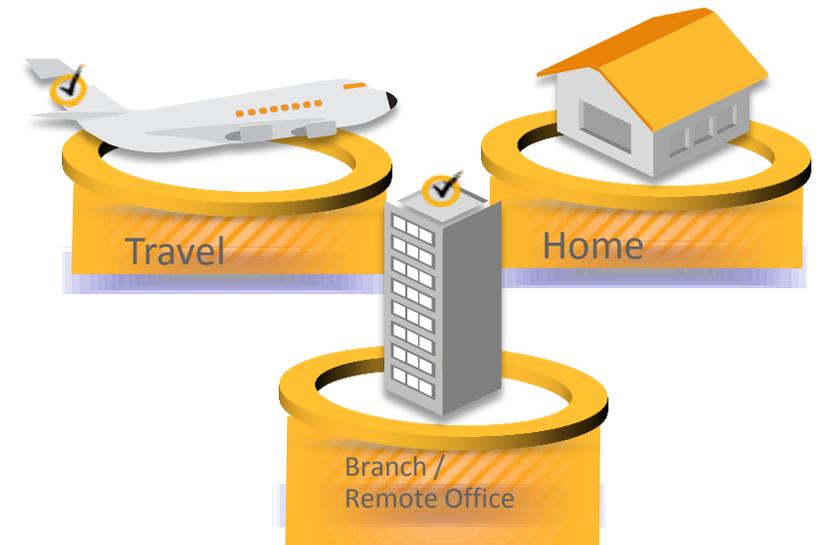




# Introduction to Cloud Enabled Management

# The Digital Nomad

- Devices used by users with no connection to the LAN or VPN present a challenge
  - Traveling employees
  - Employees working from home
  - Remote branch offices/sites
  - Devices managed remotely by Managed Service Providers (MSPs)



# Why Cloud-enabled Management (CEM)?

- **Cloud-enabled Management allows you to manage endpoints on the Internet.**
- **IT administrators want:**
  - 100% visibility of their IT resources
  - 100% patch compliance
  - Consistent software delivery rollouts (up-to-date software, especially anti-virus software)
- **Regarding resources in the Internet, IT administrators:**
  - Do not know how many IT resources actually exist
  - Are unsure about the software usage and experience low patch compliance
  - Have software version inconsistency across their environment
- **Cloud-enabled Management overcomes these insufficiencies.**



## Benefits of Cloud Enabled Management

- Allows you to manage endpoints over the Internet
- Does not require a VPN connection
  - (Also DOES NOT replace VPN)
- Does not require exposing management servers to the Internet
- Provides enhanced security for communications
- Built-in to the Symantec Management Agent



## CeM – What ITMS 7.6 functions are Supported?

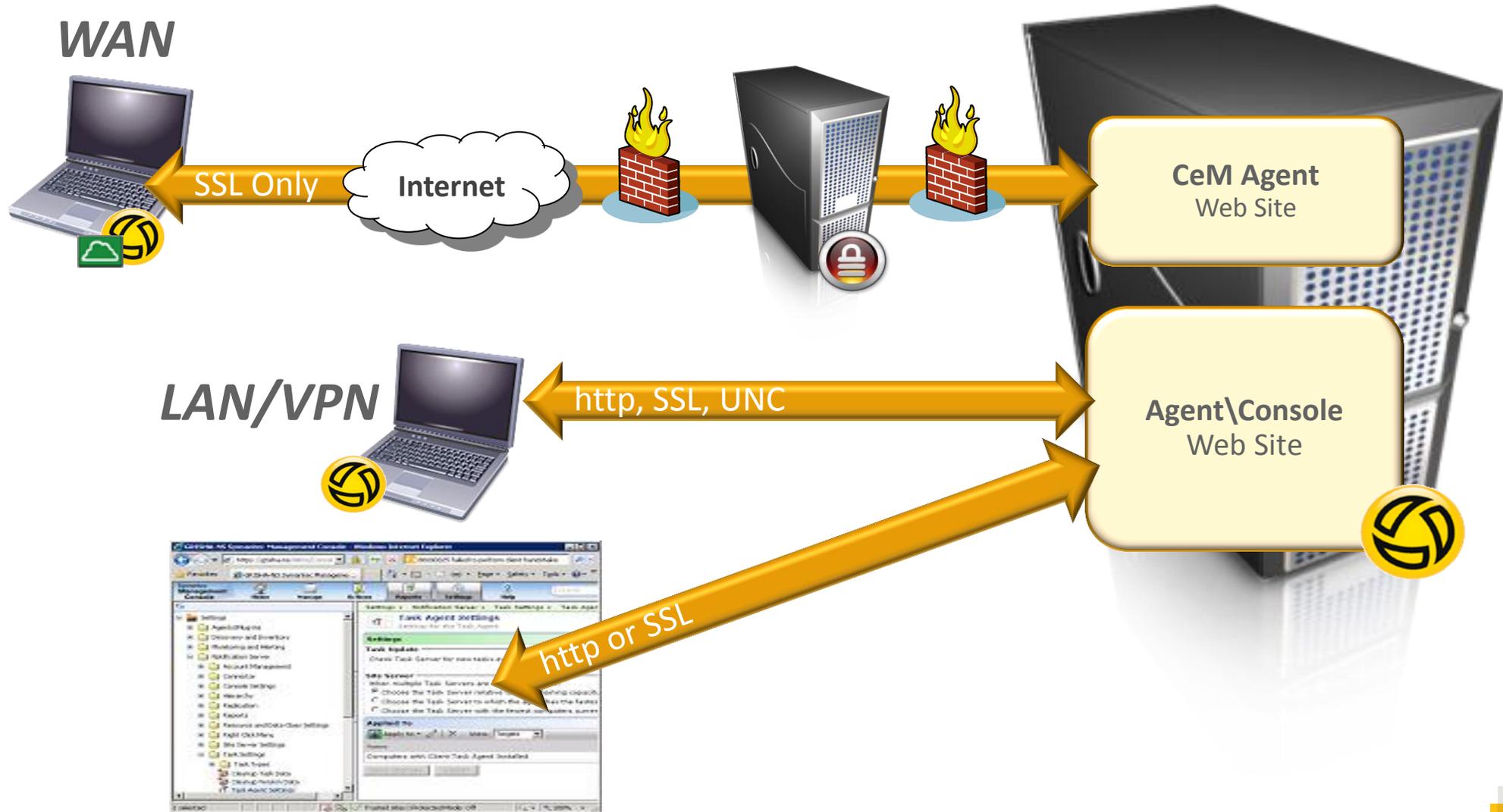


- **Windows & Mac Endpoints Supported**

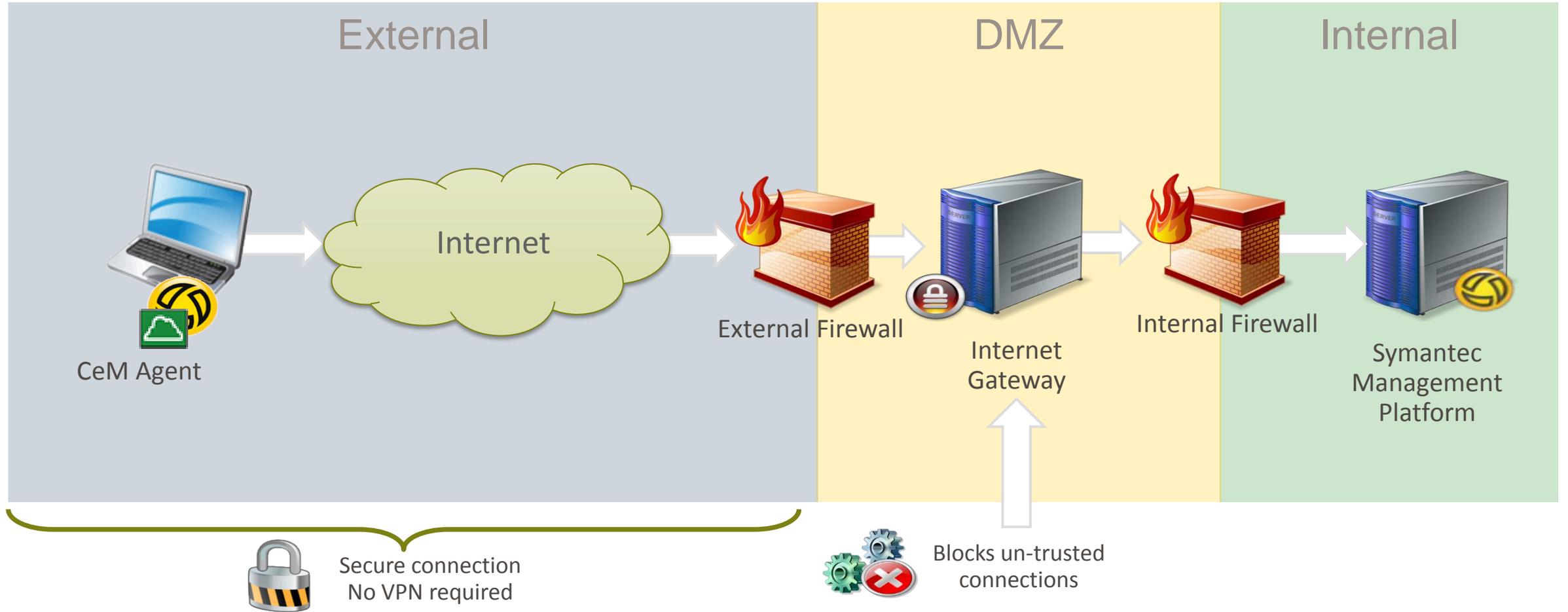
- Managed Software Delivery
- Quick Delivery (non real-time)
- Inventory Gathering
- Application Metering
- Patch Management
- Basic Client Tasks
- Hierarchy and Replication



# SMP & CeM Connectivity: Isolated Web Site Design



# Cloud Enabled Management



# Understanding Symantec Management Agent Types



- **Symantec Management Agent**

- Has been installed from the console or automation
- Expected to be on LAN or VPN Connection



- **Cloud Enabled Agent**

- SMA that has had the Cloud Enabled Feature turned ON
- Installed via CeM Agent Package OR Enabled CeM Policy



# Supported OS/Requirements



- **Symantec Management Agent**
  - Windows, UNIX, Linux, Mac OS



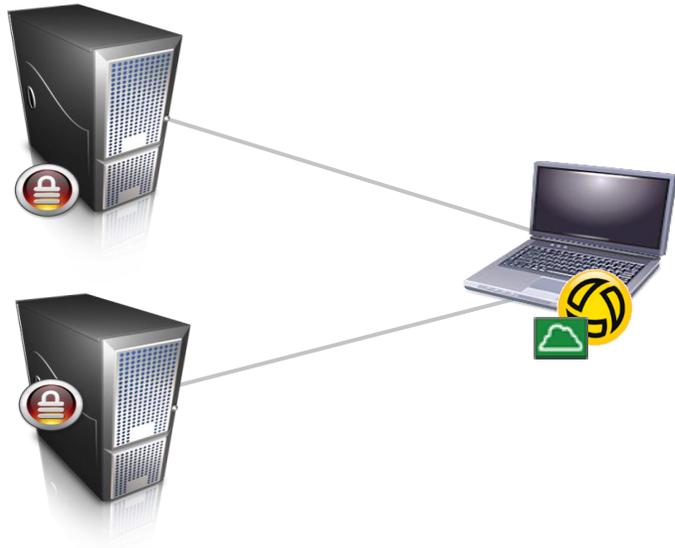
- **Cloud Enabled Endpoints**
  - Windows or Mac OS only in this release



- **Internet Gateway**
  - Physical/Virtual Server
    - 8GB RAM, 40GB HDD, Dual Core CPU, Two NICs
  - Windows Server 2008 R2 SP1 or Windows Server 2012 R2
  - .NET Framework 4.5.1 feature enabled
    - (For the IG Application Installation only)
  - Supports up to 3,000 concurrent connections



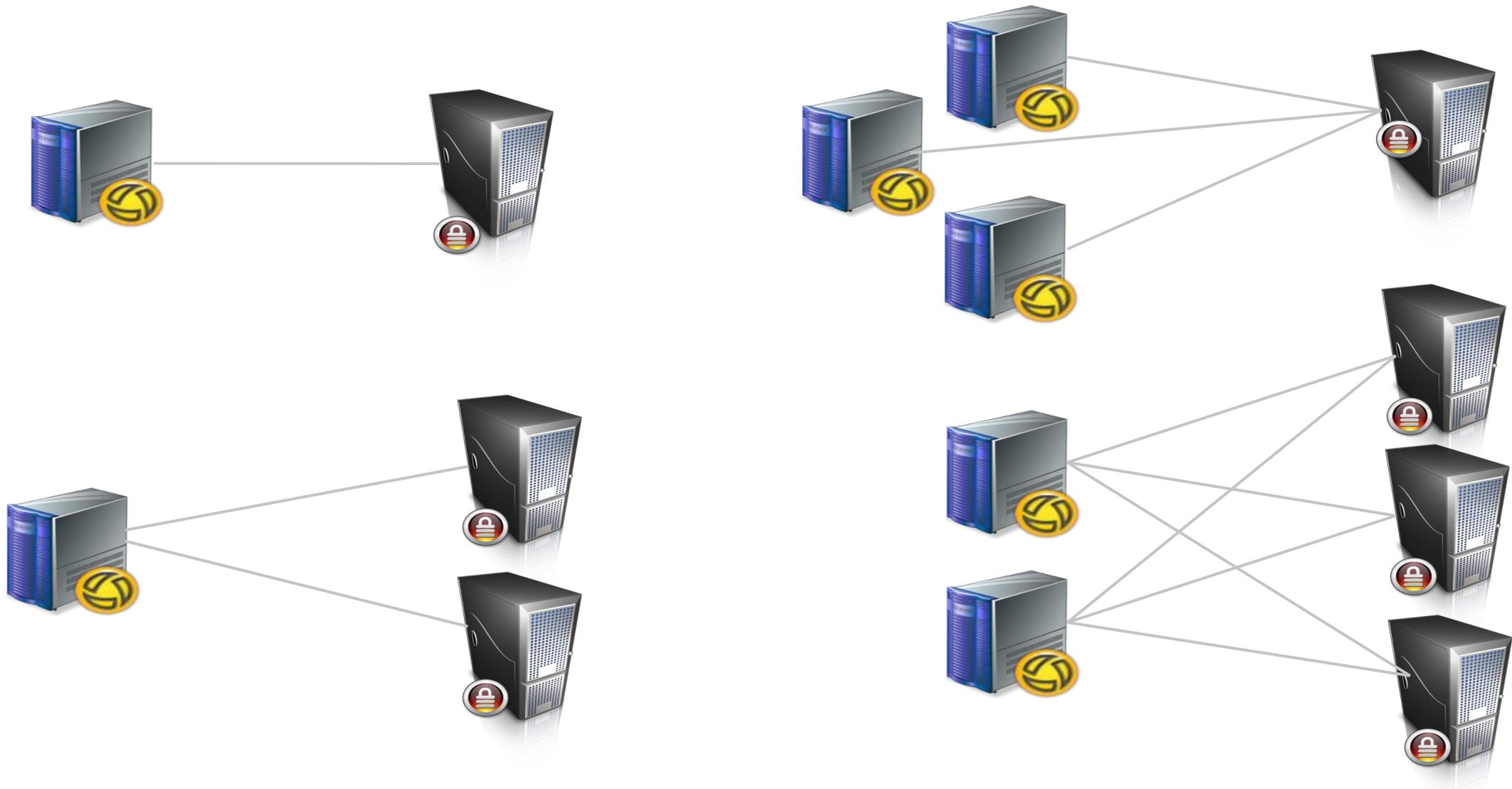
# Internet Gateway Implementation



- At least two gateways recommended
- Agents can switch between gateways
- Automatic load balancing
- All gateways are treated equal
- Automatic failover

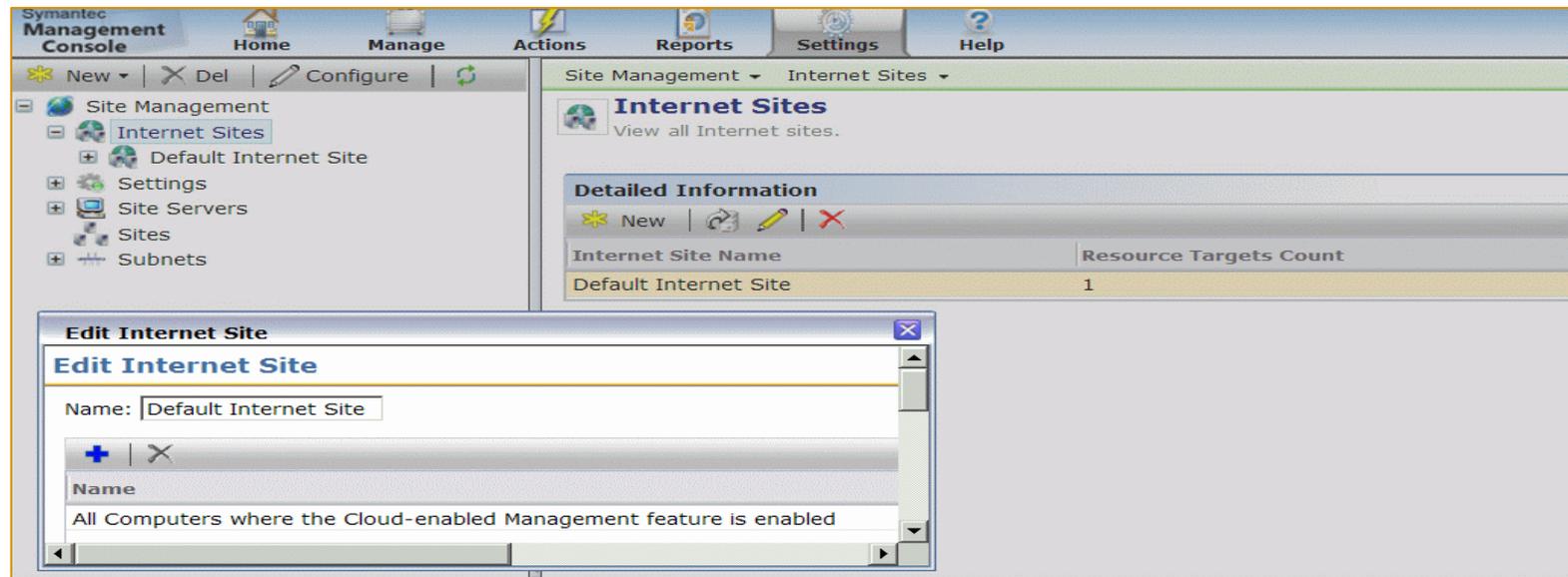


# Supported Gateway Implementations



# Internet Site Servers

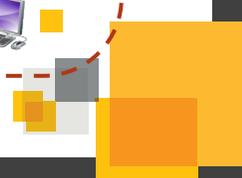
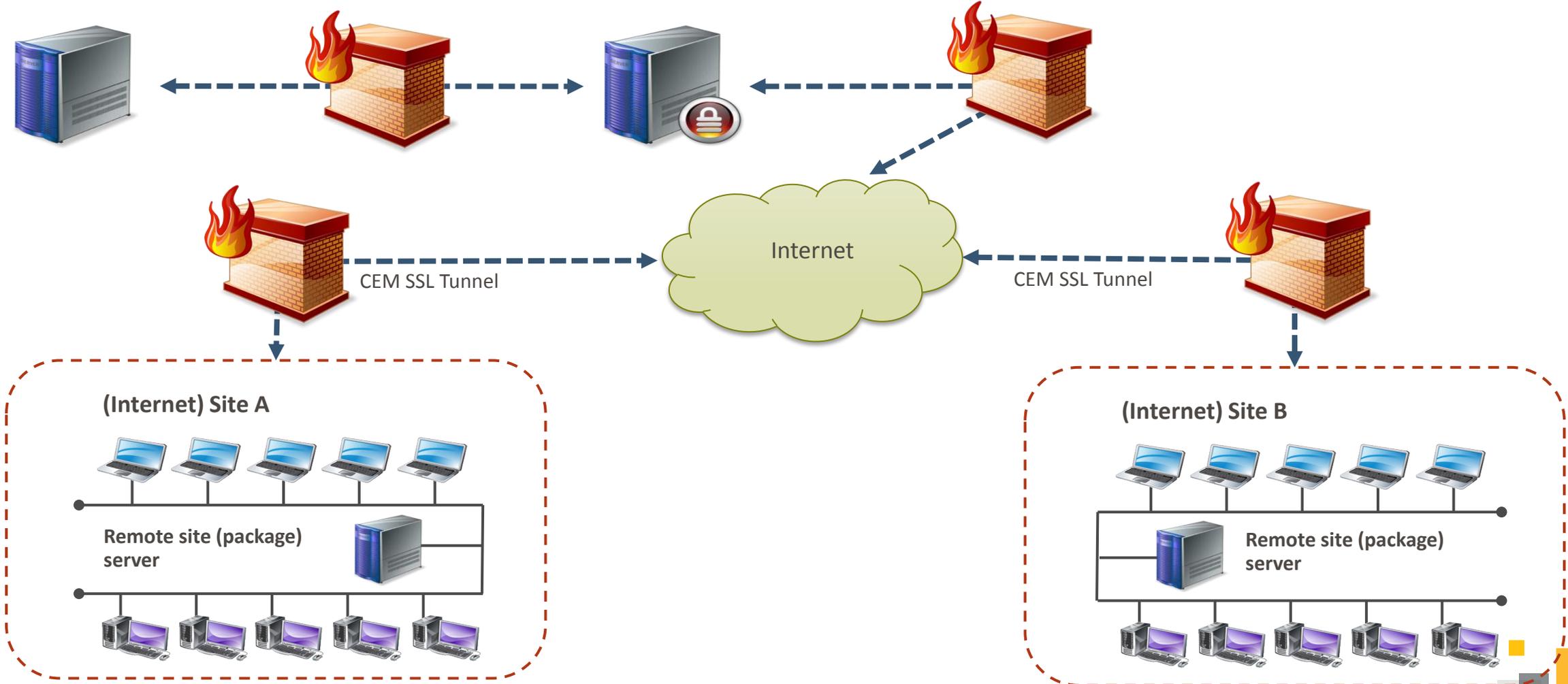
- Internet Site Servers are Site Servers that are assigned to “Internet Sites”
  - The “**Default Internet Site**” serves all CeM endpoints
    - Defined by **resource targets** instead of sites and subnets
    - Standard Site Servers can be assigned (Must be SSL!)
- Same behavior as a standard Site Servers



# Package service and CEM

Notification Server

SMP Internet Gateway





# Thank you

End of Part 1, see you after the break!