Microsoft

Эффективное управление обновлениями ПО в эпоху удаленной работы

Артём Синицын CISSP, MCSE, MCITP
руководитель программ ИБ



Программа:

- Модель выпуска обновлений для современных продуктов и сервисов Microsoft
  - Типы обновлений и пакетов их установки
  - Расписание выпуска обновлений
  - Анонс нового плана выпуска опциональных обновлений
- Обзор существующих вариантов решений для удаленного управления обновлением ПО Microsoft:
  - Windows Update
  - Windows Update for Business
  - WSUS
  - Configuration Manager
  - Microsoft Intune
- Рекомендации по использованию удаленных подключений через виртуальные частные сети VPN

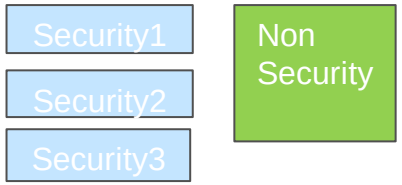
Update Tuesday



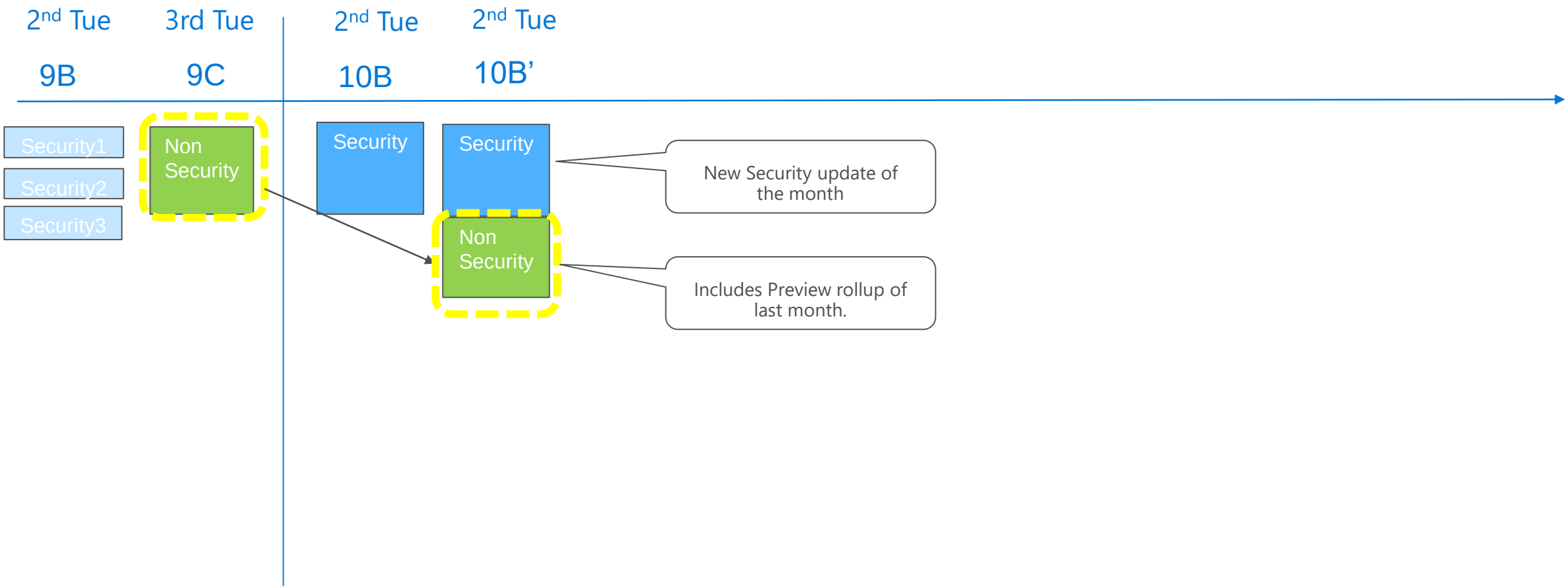
September

2nd Tue 3rd Tue

9B 9C



October 2nd Tuesday (Patch Tuesday)

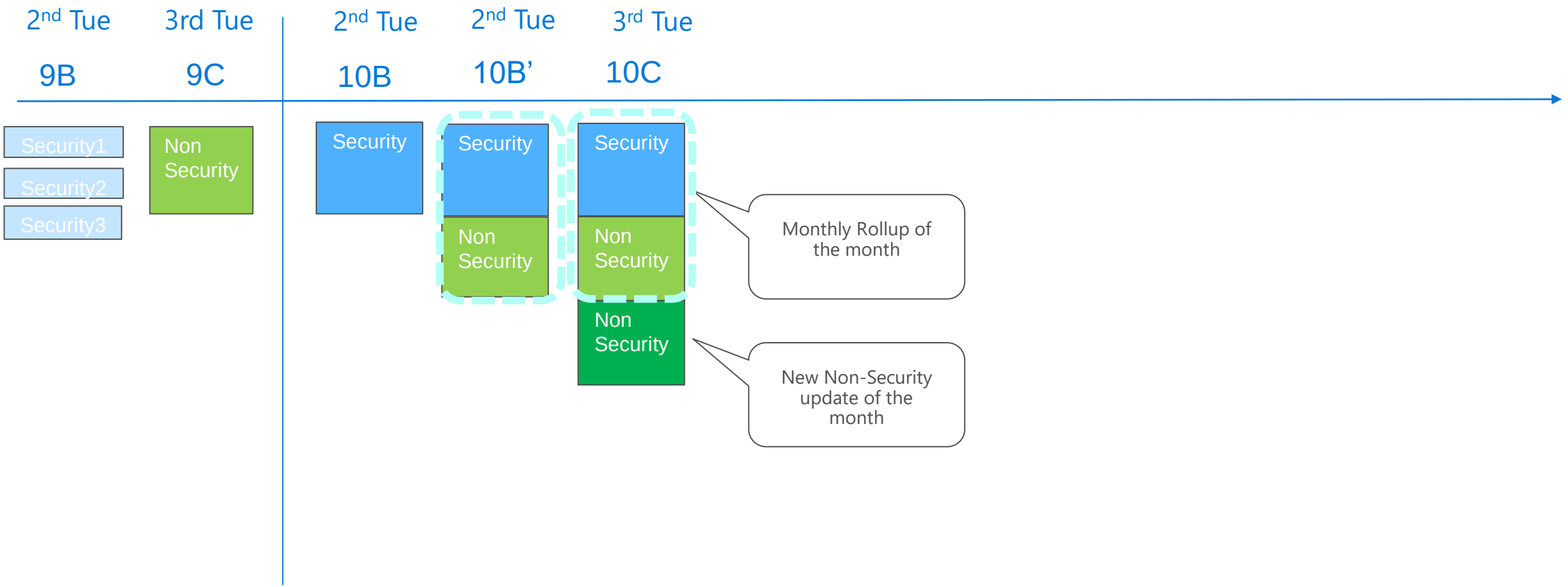


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

October 3rd Tuesday

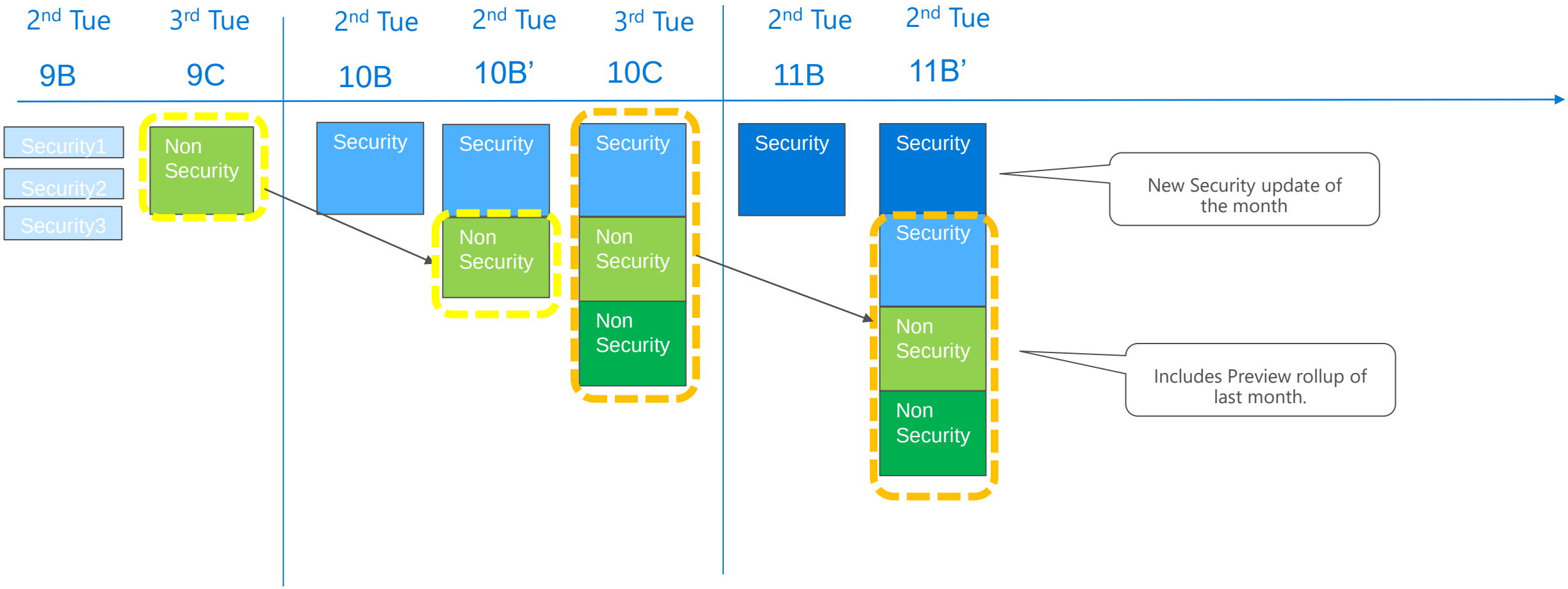


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

November 2nd Tuesday (Patch Tuesday)

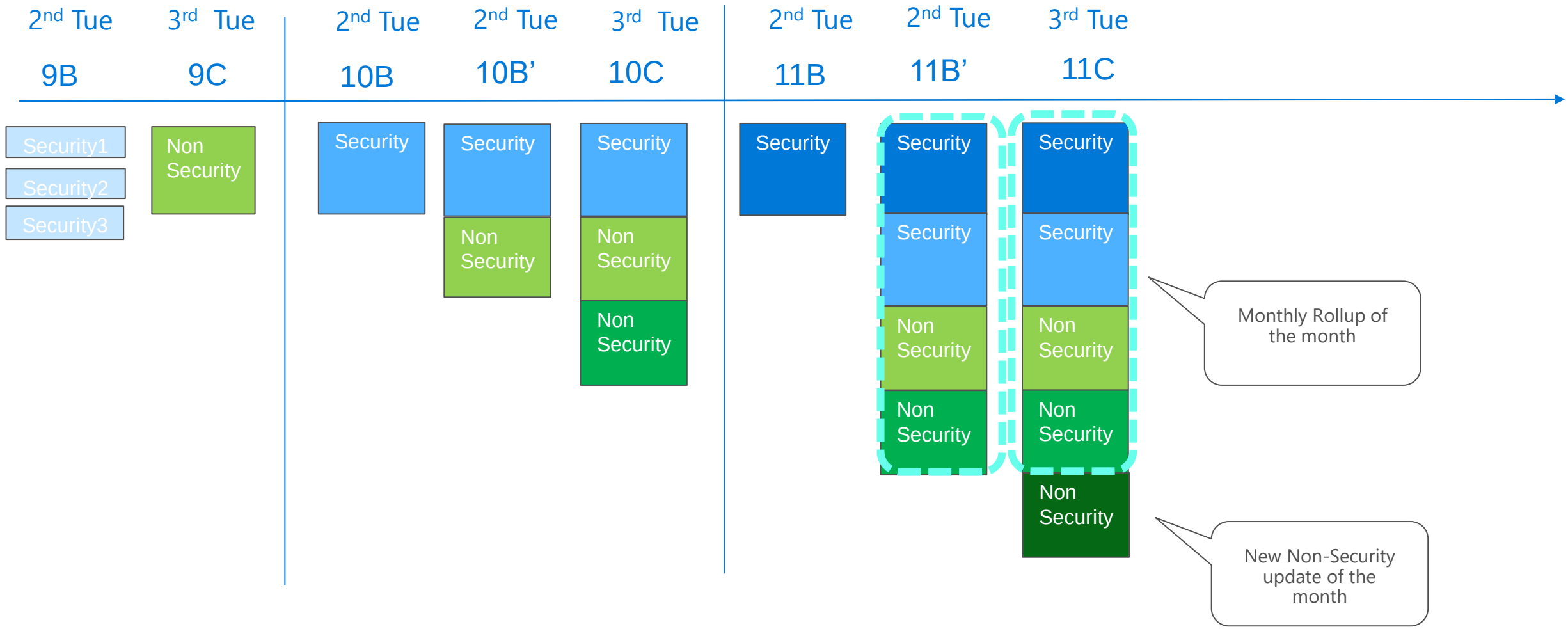


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

November 3rd Tuesday

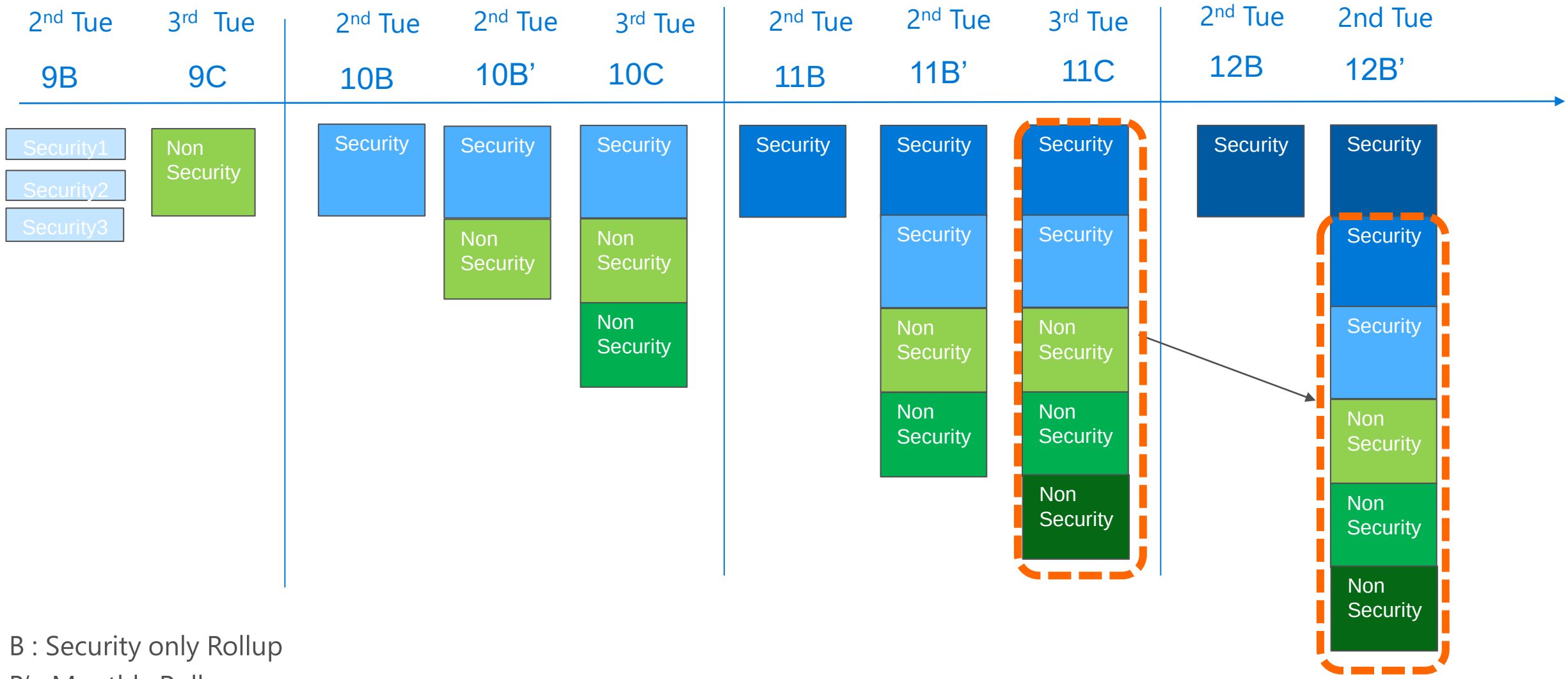


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

December 2nd Tuesday (Patch Tuesday)

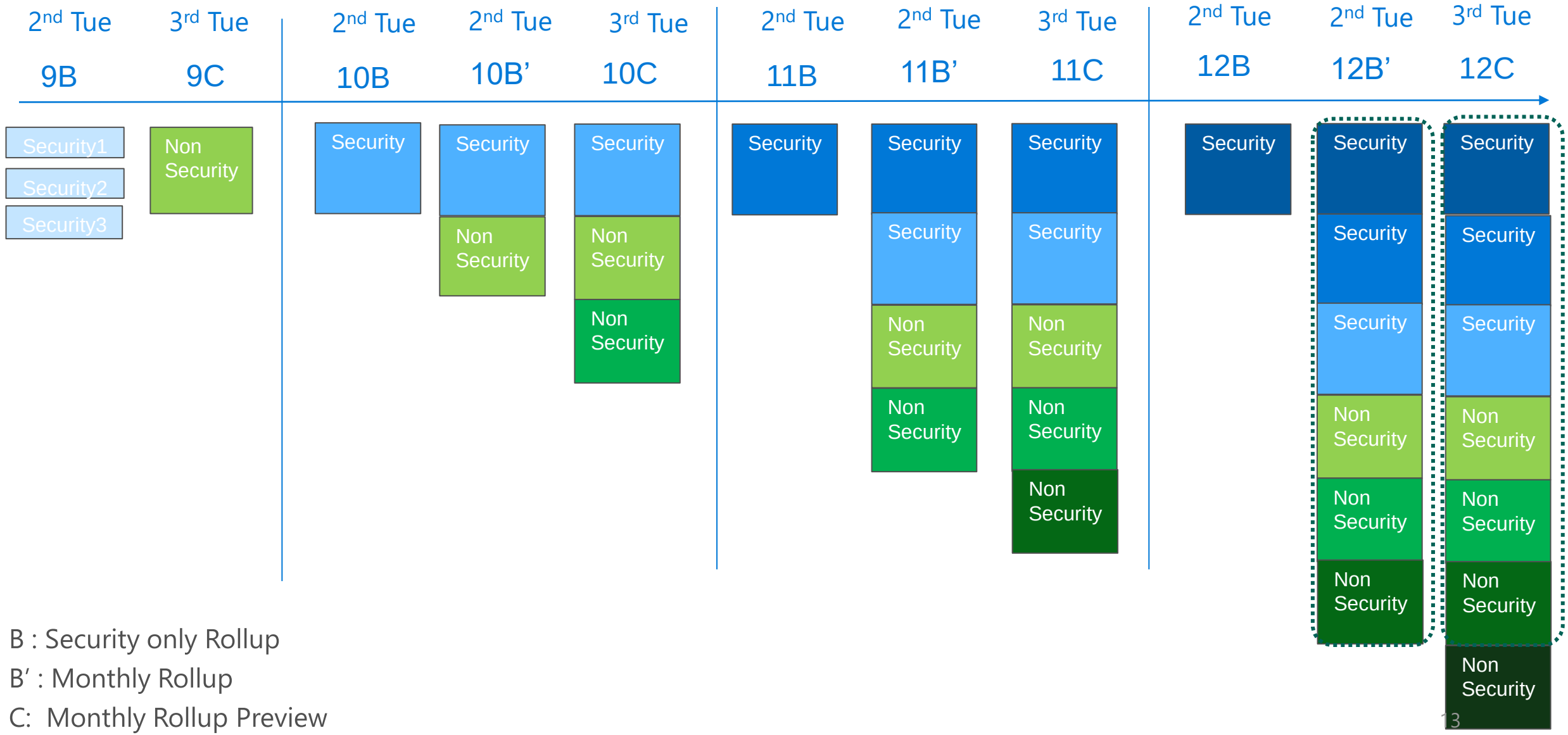


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

December 3rd Tuesday

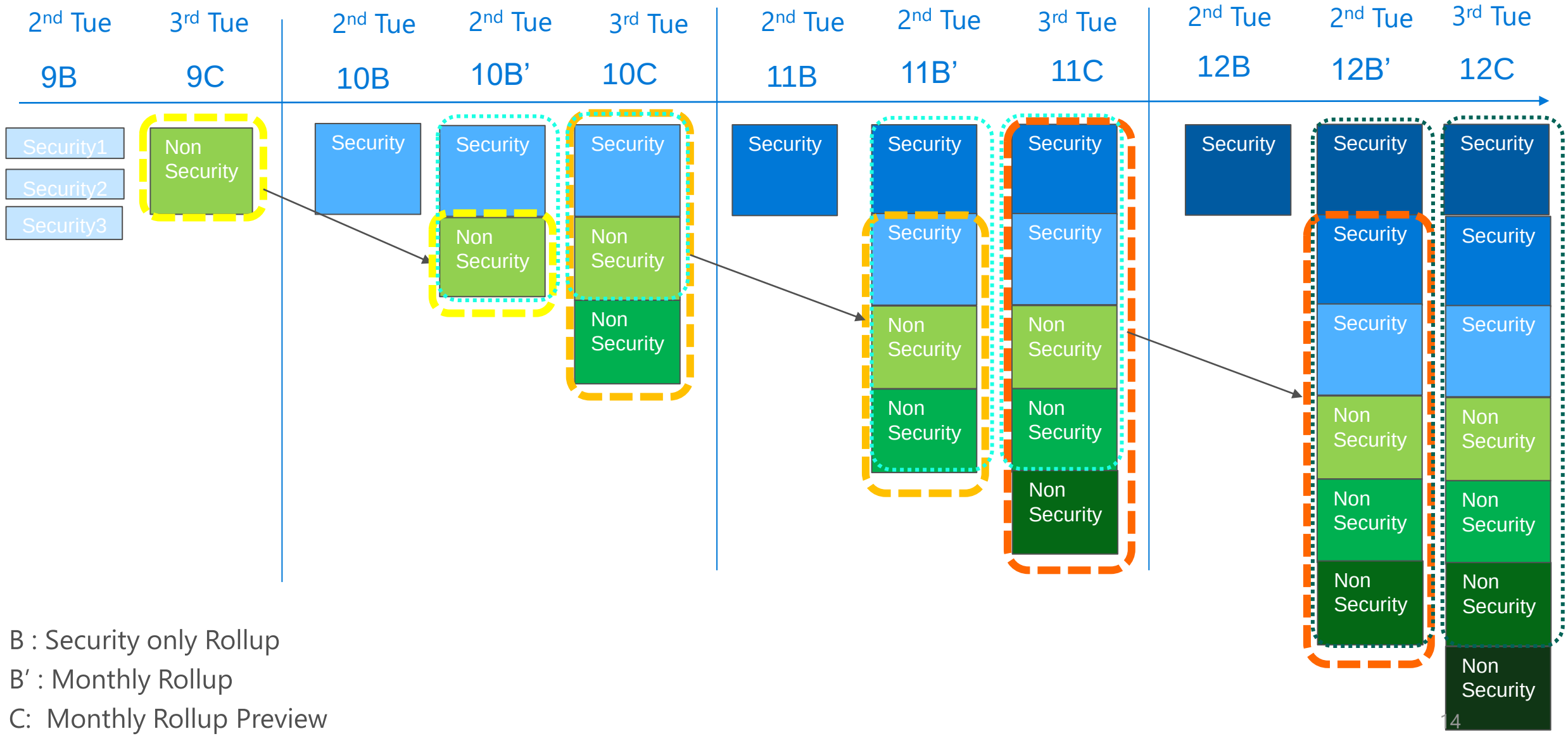


B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

Overview of update sequence



B : Security only Rollup

B' : Monthly Rollup

C: Monthly Rollup Preview

Update Package Types

Release	Type	Example of Package Title	Target Users	Distribution Channel
B	**Security Only Update**	[October, 2016] Security Only Quality Update for [OS] (KBxxxxxxx)	• For Enterprise users • Rollup that includes only the security patches for that month	• WSUS • Microsoft Update Catalog
B’	**Monthly Rollup**	[October, 2016] Security Monthly Quality Rollup for [OS] (KBzzzzzzz)	• For all users • Rollup that includes Security update + non-security updates	• Windows Update • WSUS • Microsoft Update Catalog
C	**Monthly Rollup Preview**	[October, 2016] Preview of Monthly Quality Rollup for [OS] (KBnnnnnnn)	• For all users • Rollup that includes fixes of B' + new non-security fixes • Optional distribution	• Windows Update • WSUS • Microsoft Update Catalog

Upcoming Windows optional updates

Microsoft announced a pause in the release of all optional non security updates (C and D updates):

"We have been evaluating the public health situation, and we understand this is impacting our customers. In response to these challenges we are prioritizing our focus on security updates. Starting in May 2020, we are pausing all optional non-security releases (C and D updates) for all supported versions of Windows client and server products (Windows 10, version 1909 down through Windows Server 2008 SP2).

***There is no change to the monthly security updates** (B release – Update Tuesday); these will continue as planned to ensure business continuity and to keep our customers protected and productive."*

Source: https://docs.microsoft.com/en-us/windows/release-information/windows-message-center#405

Possible alternatives for updates

Options	Implementation difficulty	Implementation time
Windows Update	✪	◔
Windows Update for Business	✪	◔
WSUS	✪✪ (Configuration change)	◔
Intune	✪✪✪	◕ From few minutes to several days
Configuration Manager	✪✪✪✪ or more depending on the current setup	● From some hours to several days

Legend

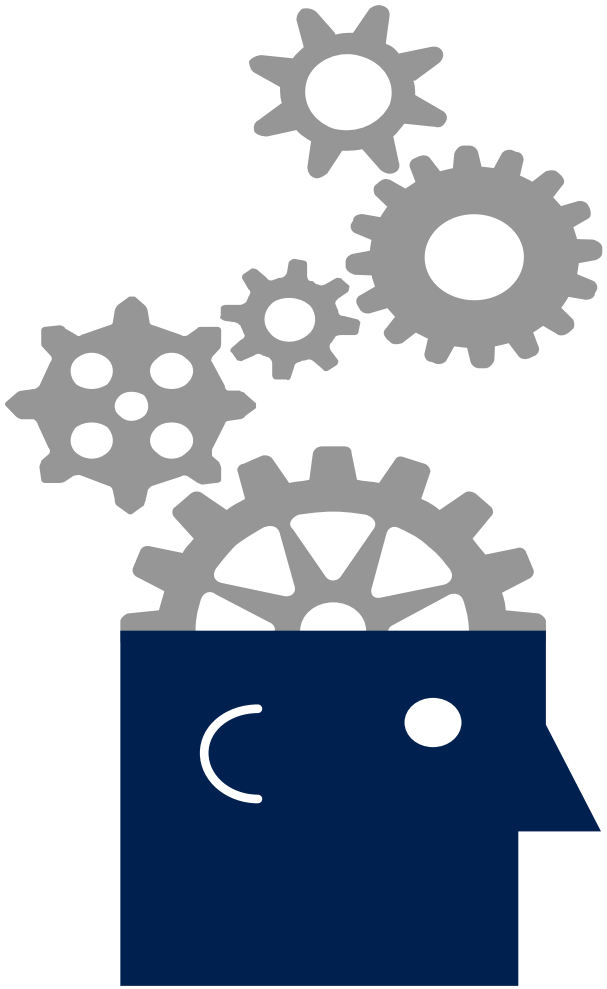
Difficulty (1 star – easy, 5 stars – complex) ✪

Time (from few minutes to several days) ◔ ◔ ◑ ◕ ◕ ●



Windows Update

Difficulty
Time



Advantages

- Available for all the supported Windows versions.
- Windows updates available immediately.
- No impact on VPN bandwidth if the client VPN is configured in “split-tunnel”*.

Disadvantages

- No control and no available reporting*.
- If there is no “split-tunnel”* all the network traffic continues to go through the VPN.

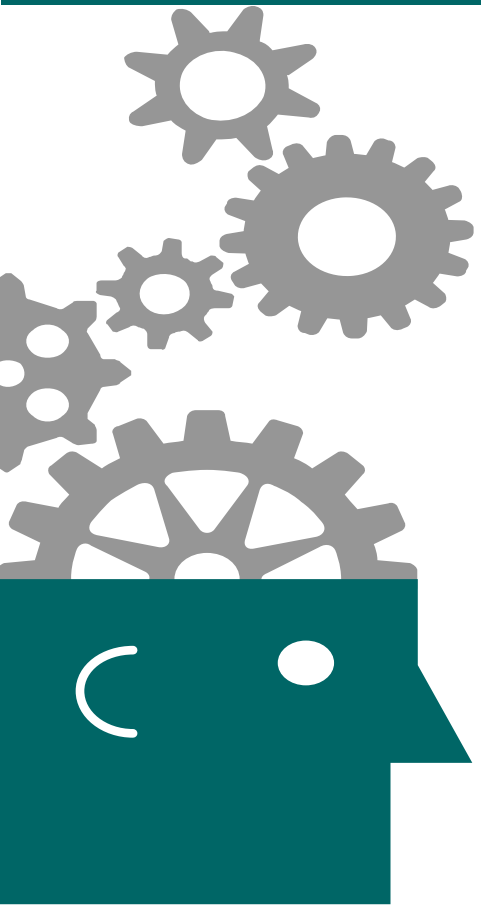
Comments

* Allows differentiation of internet flow from corporate traffic to avoid impacting VPN.

- Machines need to have this GPO Not configured or disabled -> *Do not connect to any windows update internet locations*

Windows Update for business

Difficulty
Time



Advantages

- Available for all the supported Windows 10 Pro, Ent, Edu & Windows Server 2016+.
- Windows updates available immediately.
- No impact on the VPN bandwidth if the client VPN is configured in “split-tunnel”*.
- Additional Group Policies/GPO.

Disadvantages

- No control and no available reporting.
- If there is no “split-tunnel”* all the network traffic continues to go through the VPN.

Comments

* Allows differentiation of internet flow from corporate traffic to avoid impacting VPN.

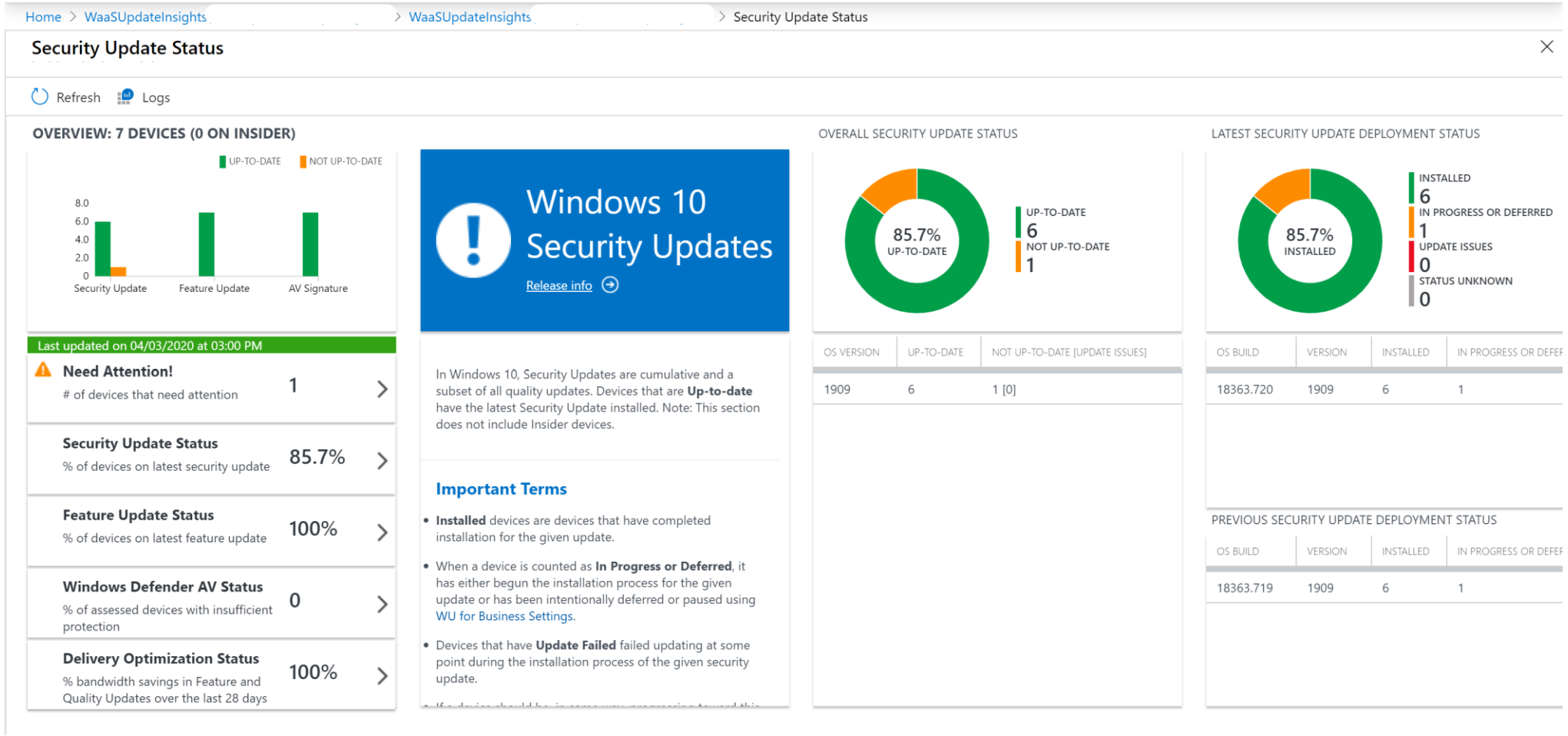
- Machines need to have this GPO Not configured or disabled -> *Do not connect to any windows update internet locations*

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

Windows Update for business

Difficulty
Time

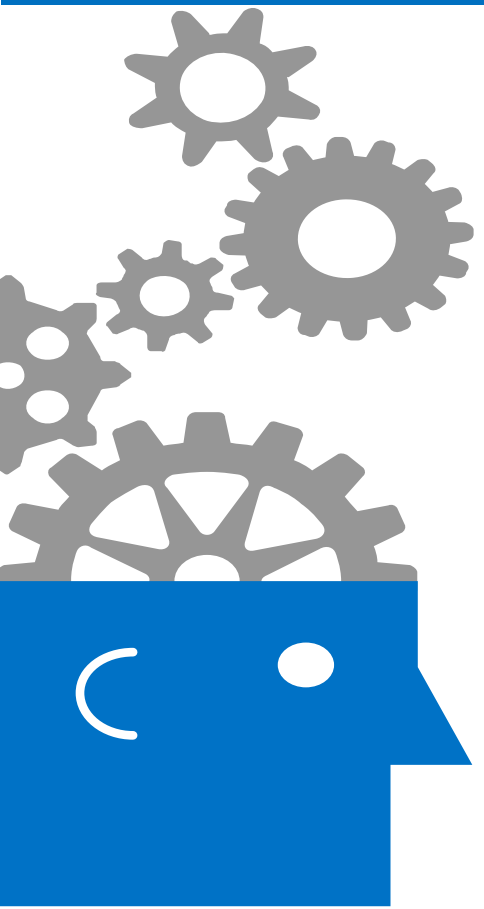




https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-monitor

WSUS

Difficulty
Time



Advantages

- Possibility to force the clients to download update binaries from Windows Update by keeping the control and the reporting in WSUS.
- Very quick change on the WSUS server, easy to go back.
- Low impact on the VPN bandwidth if the client VPN is configured in “split-tunnel”*.

Disadvantages

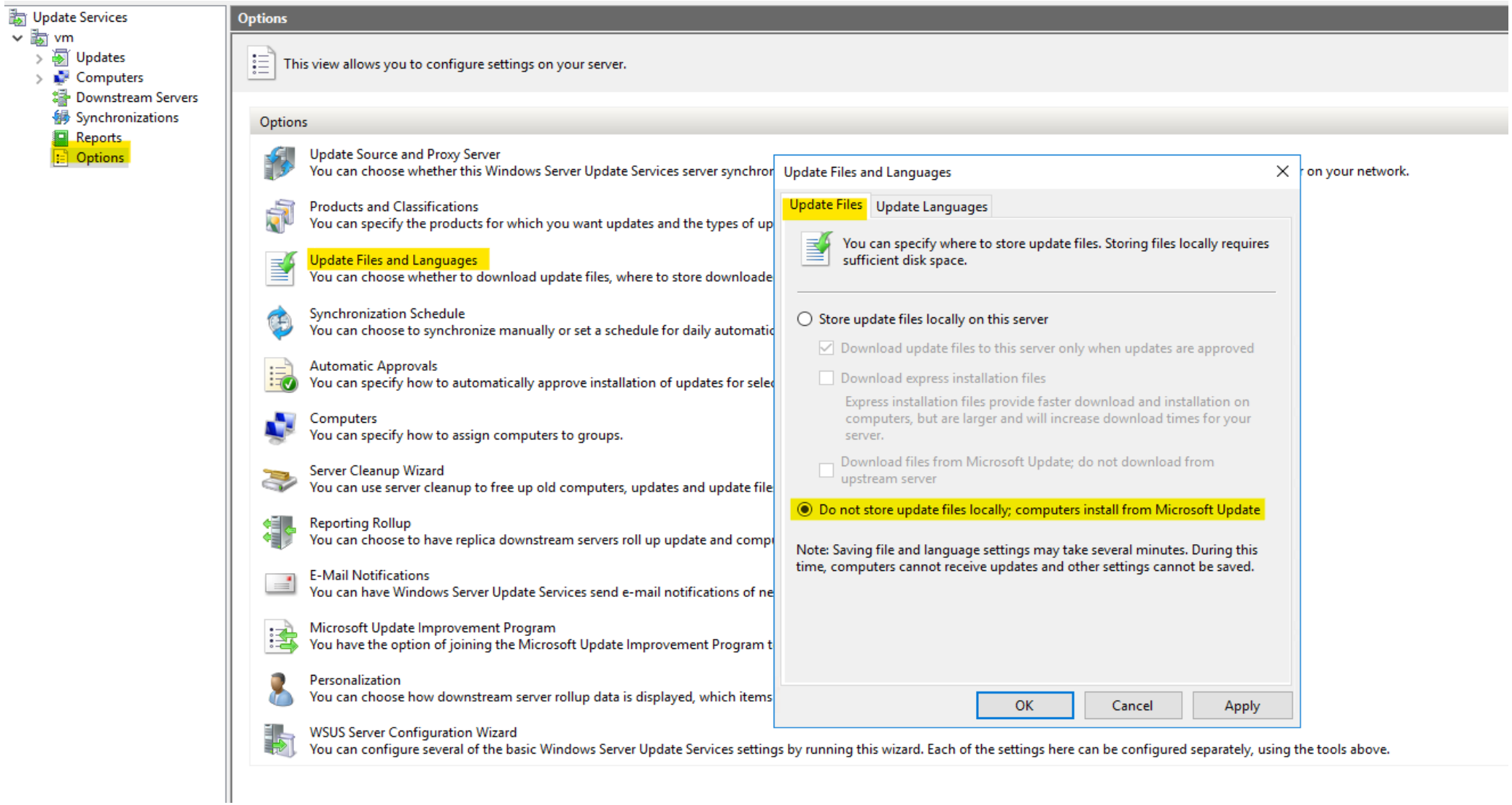
- All the clients of the WSUS server will download binaries from the same source, including the machines left on the LAN (servers).
- If there is no “split-tunnel”* all the network traffic continues to go through the VPN.

Comments

* Allows differentiation of internet flow from corporate traffic to avoid impacting VPN.

- Machines need to have this GPO Not configured or disabled -> Do not connect to any windows update internet locations

If the WSUS infrastructure is already in place and the VPN client allows the split-tunneling, modify the WSUS server settings as follows:



WSUS

Intune

Difficulty
Time



Advantages

- Works out-of-the-box (no infra on-premise need).
- Direct communication with Microsoft Update.
- Possibility of cohabitation between Intune and Configuration Manager by using the co-management.
- Easy and fast configuration and implementation.
- No impact on the VPN bandwidth if the client VPN is configured in “split-tunnel”* or if only internet access.

Disadvantages

- Less granular deployment possibilities than with Configuration Manager or WSUS on premise (no deep management of updates or fixed deployment date).
- The clients must be linked to AzureAD and Intune, this can require a certain implementation effort (Hybrid AzureAD join…).
- If there is no “split-tunnel”* or internet access, all the network traffic continues to go through the VPN.

Comments

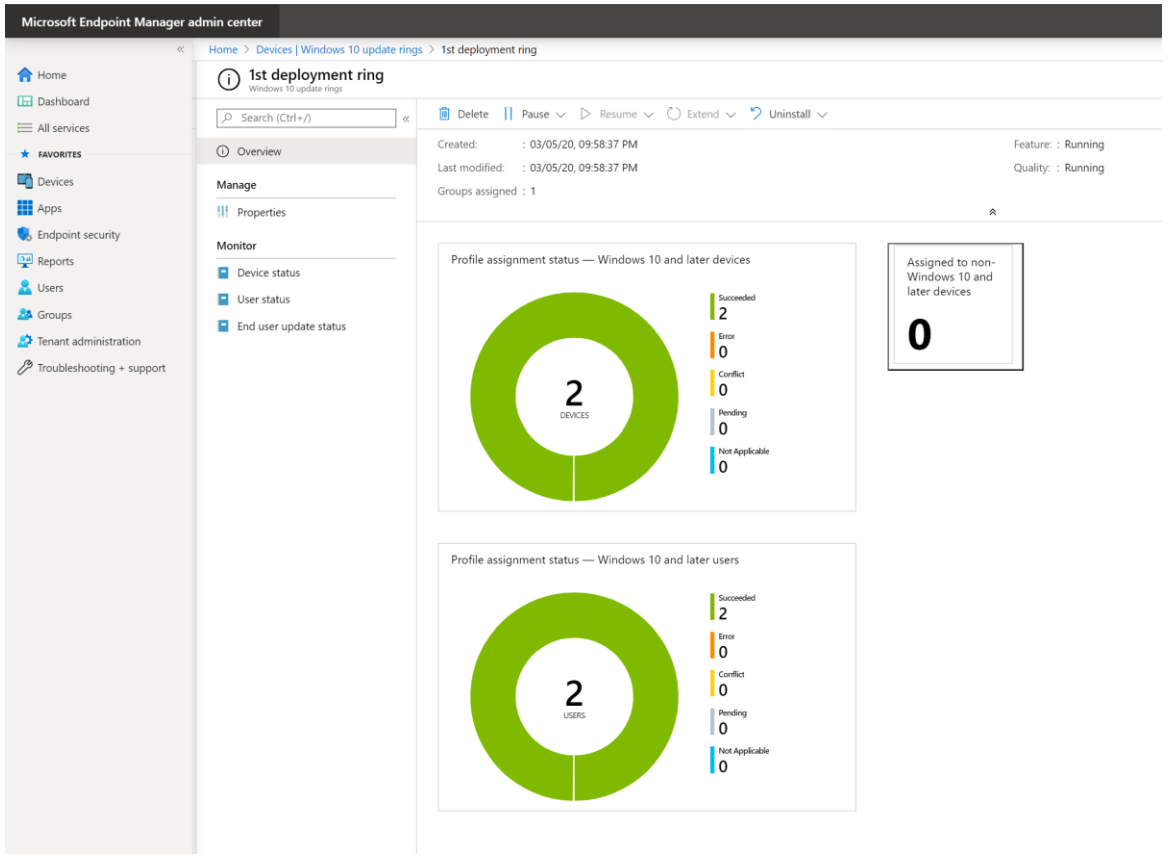
Intune allow for the easy configuration of the Windows Update for Business policies on the client workstations with a unique and simple setting.

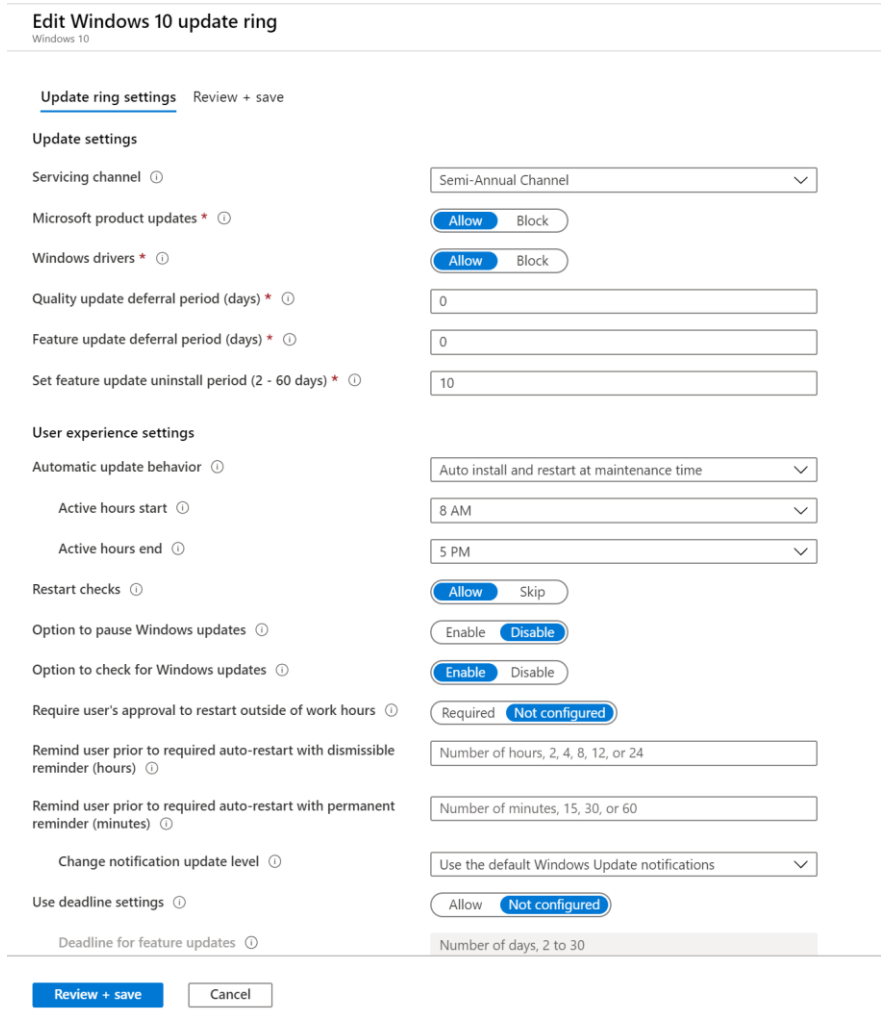
*Allows differentiation of internet flow from corporate traffic to avoid impacting VPN.

Intune

Effort
Time







Configuration Manager

Effort ✪✪✪
Time ●



Advantages

- Wave volume control by precise targeting of client workstations across multiple collections.
- Management of the deployment phases
- Distribution and compliance reporting.
- Ability to configure the download of binaries through Microsoft Update.

Disadvantages

- Requires upstream preparation of the resources required for deployments.
- Relatively long required time depending on the infrastructure already in place.

Comments

The configuration choices are important:

- IBCM (Internet Based Client Management).
- CMG (Cloud Management Gateway).
- VPN Split Tunneling.

The number of waves will be defined by the VPN maximum capacity.

The Windows 10 VPN Client Platform

Consistency Across Desktop and Mobile SKUs

- Unified Platform Development (architecture and binaries)
- Consistent UI and Connection Experience

Open Partner Platform

- Open to all VPN ISVs
- Publish One App for both Desktop and Mobile Platforms

Consistent Deployment Method for Desktop and Mobile SKUs

- Connection Profile Deployment using MDM Solutions such as Microsoft Intune

Impressive Client-Side Feature Set

- Always-On Auto-Connect VPN
- App Triggers and Traffic Filters
- LockDown VPN and More

Always-On (Auto-Connect) VPN

VPN Auto-Connection

- Automatically connect to corporate resources from remote locations
- Works with Single Sign-On (SSO) options

Network Detection

- *Trusted Network Detection* identifies remote corporate network
- No special infrastructure requirement
  EX: A Network Location Service (NLS)

User Experience

- User can manually disconnect connection
- User can easily disable auto-connect behavior if desired

A Platform Capability

- Plugin architecture means that third-party client plugins require no special coding or awareness to leverage Always-On

VPN App-Triggers

VPN App-Triggers

- VPN connection established when an administratively defined *trusted app* is launched

App-Triggers

- Desktop Apps (using binary path)
- Store Apps (using package family name)
  Example: Microsoft.ZuneMusic_2.0.132.0_x64__8wekyb3d8bbwe

Granular Traffic Control

- By default, all applications are permitted to communicate across the VPN tunnel
- Use in conjunction with *traffic filters* to implement additional restrictions

Per App Tunnel Mode

- Use with *traffic filters* to add set tunnel mode behaviors per application
- Split or forced tunnel modes

VPN Traffic Filters

VPN Traffic Filters

- Controls traffic permitted to traverse the VPN interface
- Traffic filter list are plumbed to the Windows Filtering Platform (WFP)

Filter Parameters

- Local and/or remote IP ranges
- Local and/or remote port ranges
- Protocol type (IPv4/IPv6)

Filtering Extras

- *App ID* can also be used as a parameter
- A *Routing Policy Type* can be used to assign a tunneling behavior to the filter

Filter Processing

- Boolean AND for filter parameters
- Boolean OR for stacked rules
- Default *deny all* terminates filter list

LockDown VPN

LockDown VPN

- For extremely security conscious organization
- Settings: ON or OFF

LockDown Behavior

- Is an *Always-On* profile
- *Cannot* be disconnected
- *All* traffic is tunneled (forced-tunnel)

LockDown Behavior (cont.)

- No active VPN connection means *no* network connectivity
- No other VPN connection profiles can be connected or modified

Filter Exceptions

- Protocols necessary to establish VPN connection or communicate with the MDM service
- No administrative exemptions

VPN Integration Scenarios

Enterprise Data Protection (EDP)

- Enterprise Data Protection (EDP) policies secure company data on remote devices
- VPN fully integrate with EDP with one configuration settings (EdpModeId)

Microsoft Passport

- Uses TPM to replace passwords with strong two-factor authentication
- Combine Always-On with Windows Hello for a seamless SSO experience

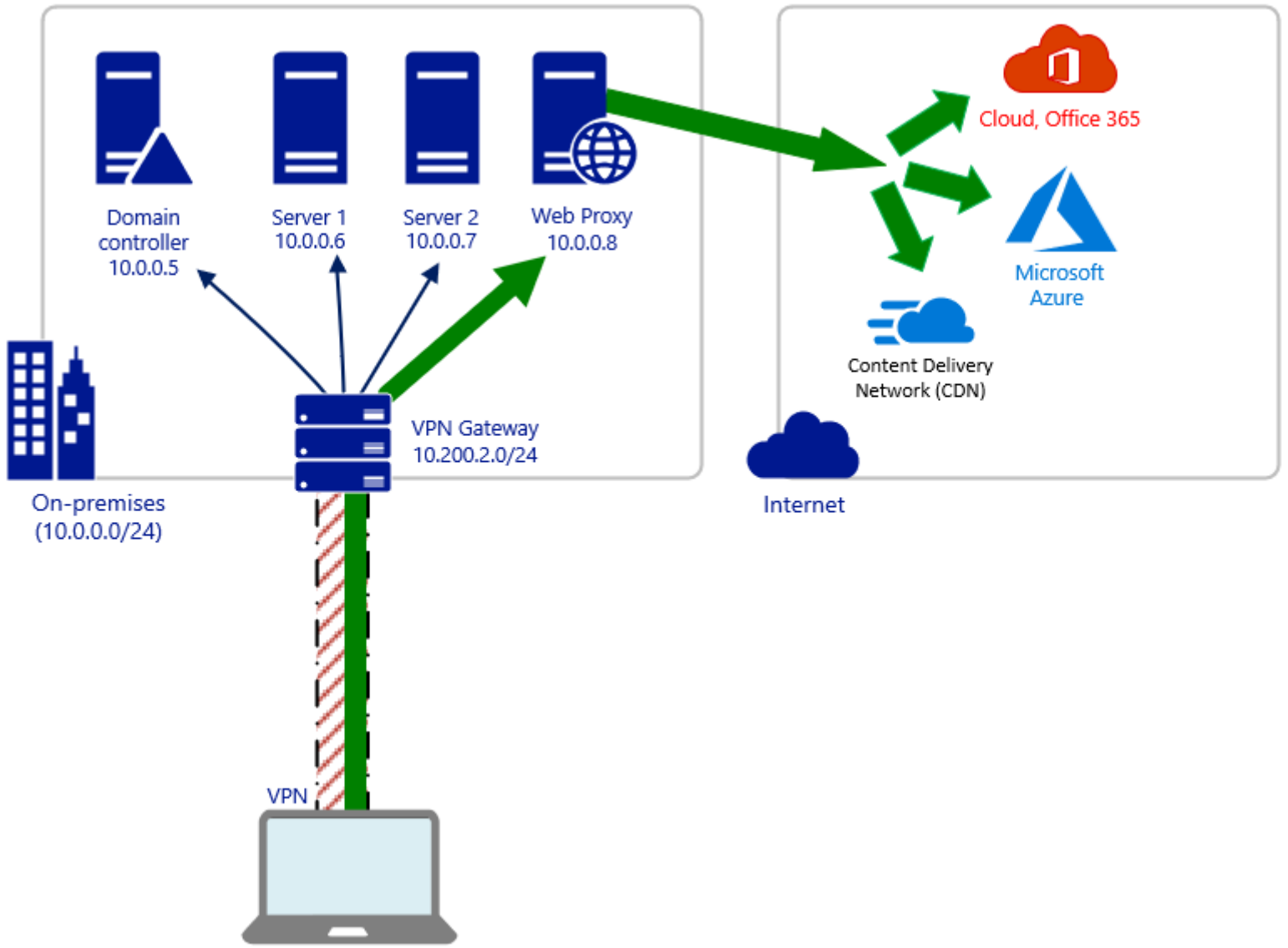
Conditional Access

- Evaluates the user login to make real-time access decisions
- Uses the Conditional Access Framework and Intune compliance policies

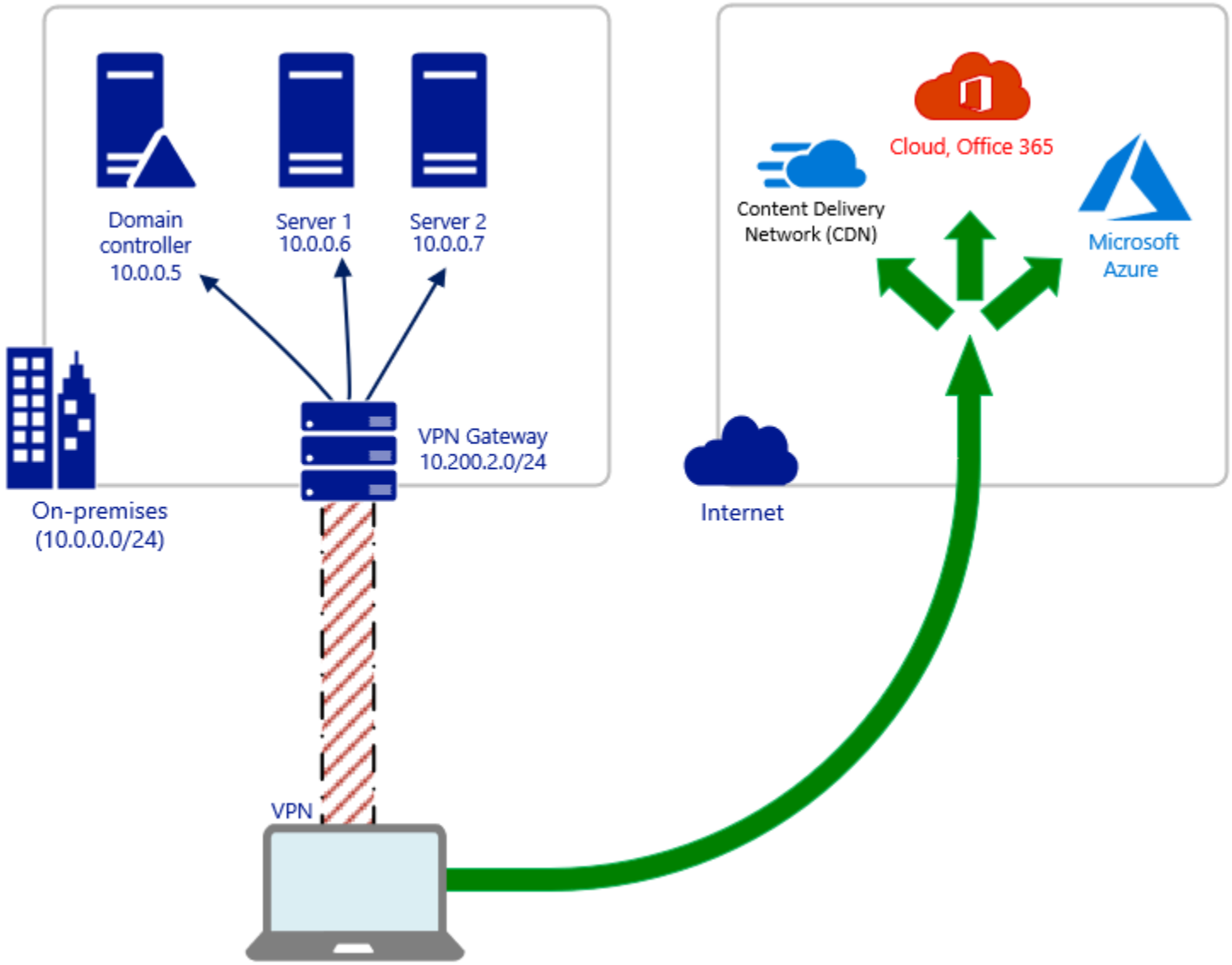
Device Compliance

- The other half of Conditional Access
- Windows Health Attestation Service: Cloud-based and new TP server role

VPN Force Tunneling



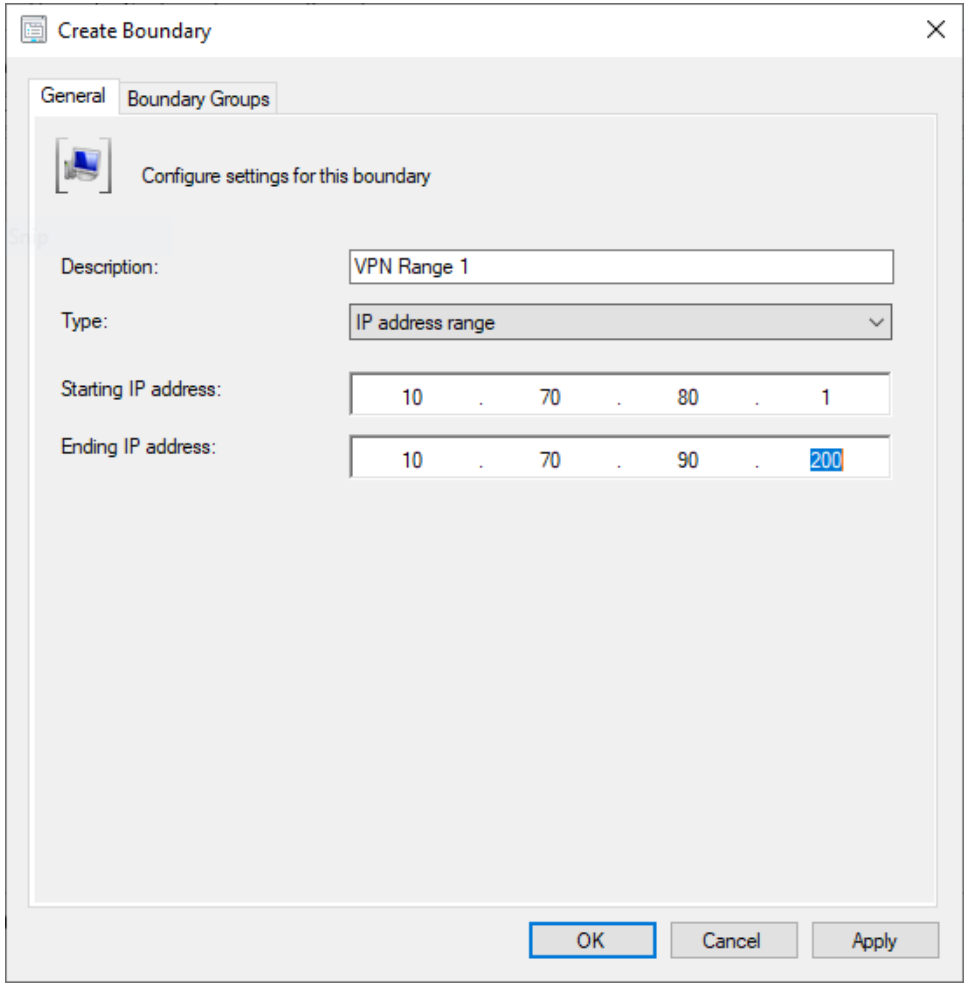
VPN Split Tunneling

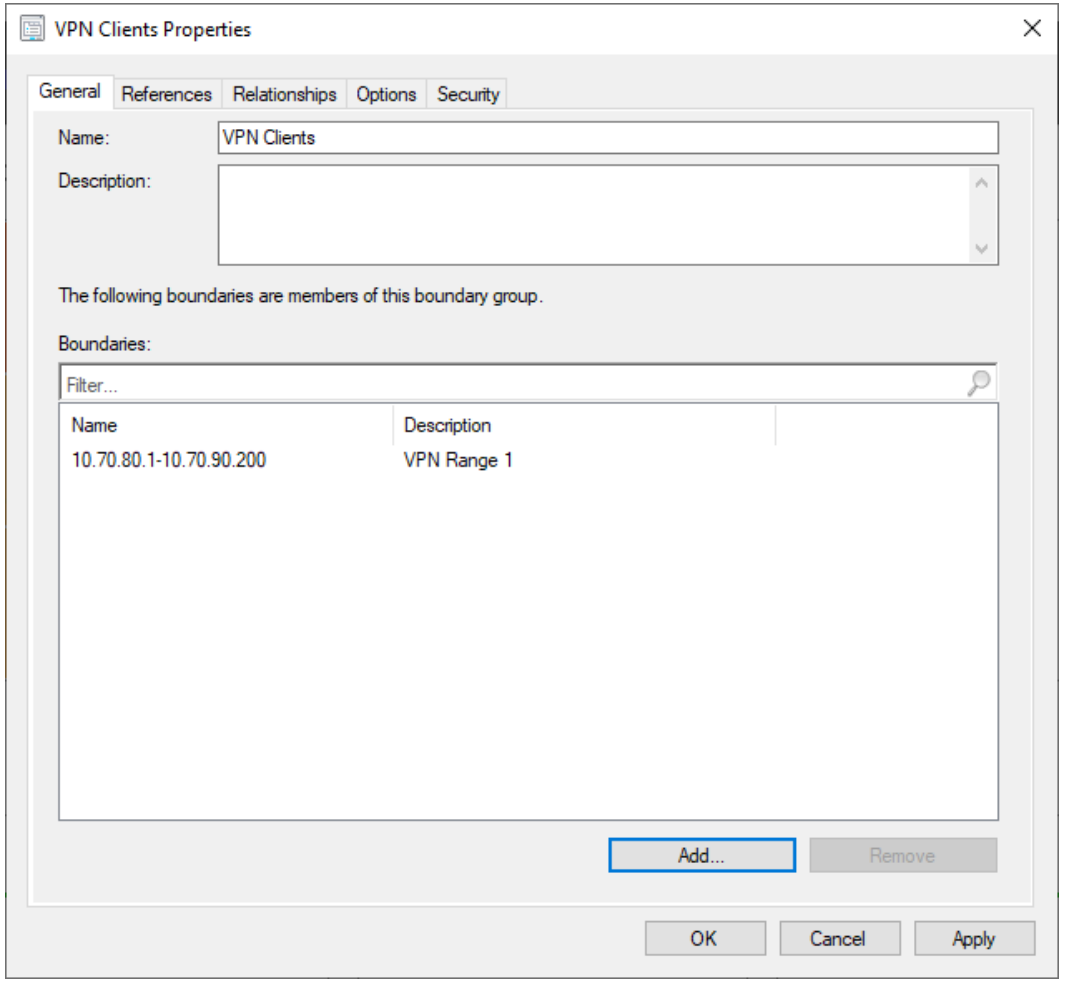


Configuration Manager

Effort
Time



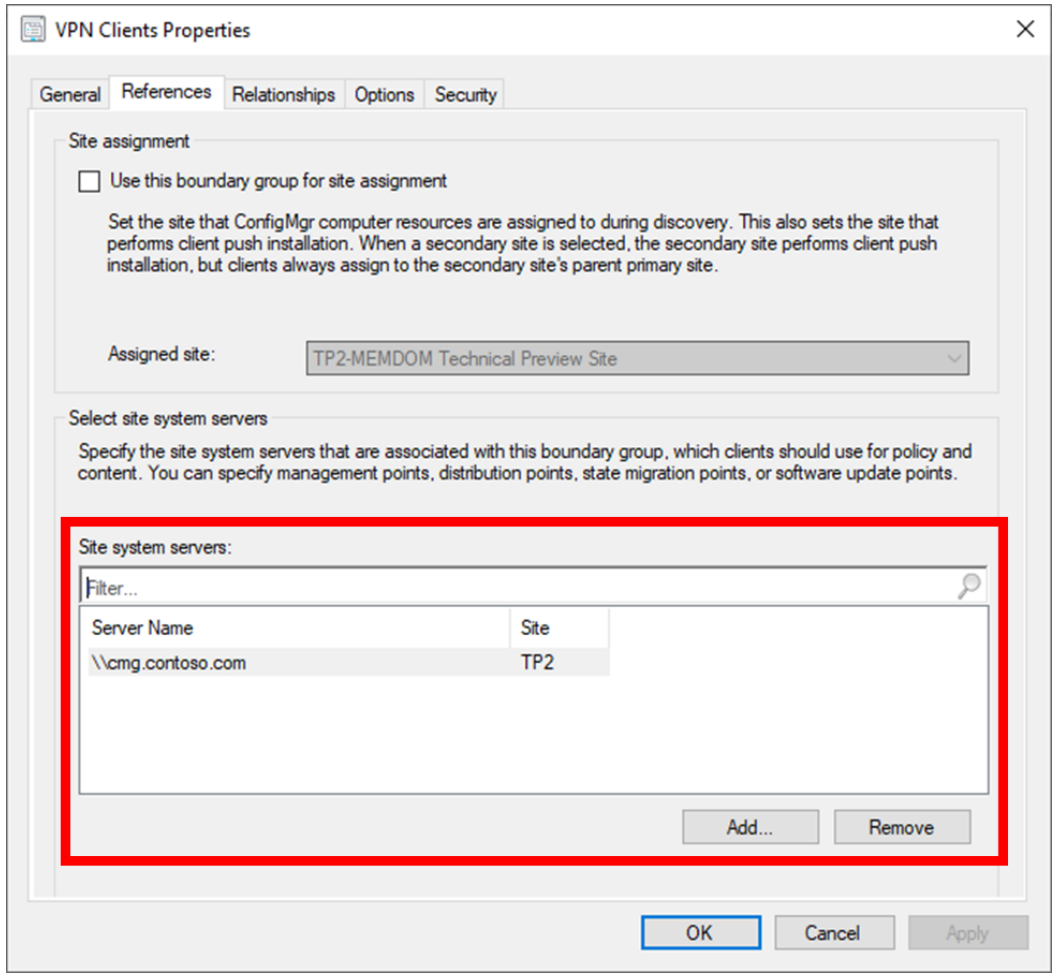


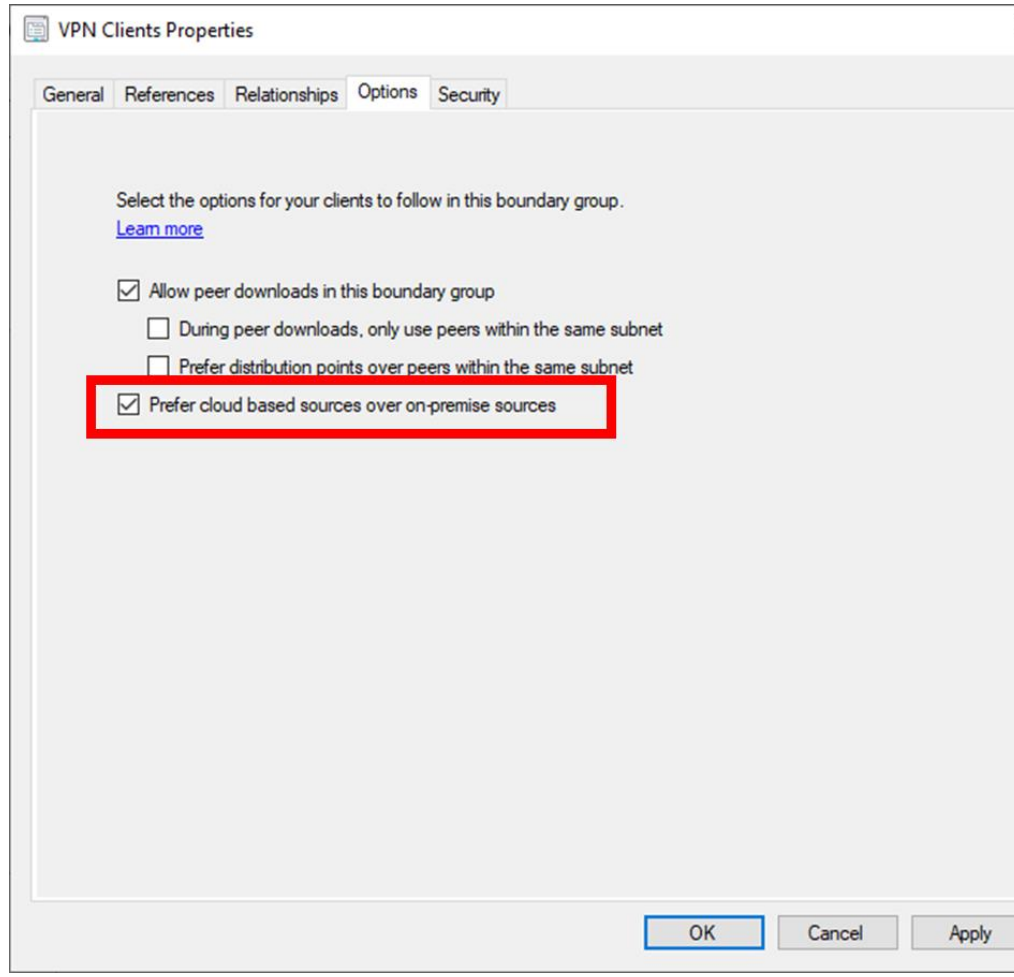


Configuration Manager

Effort
Time



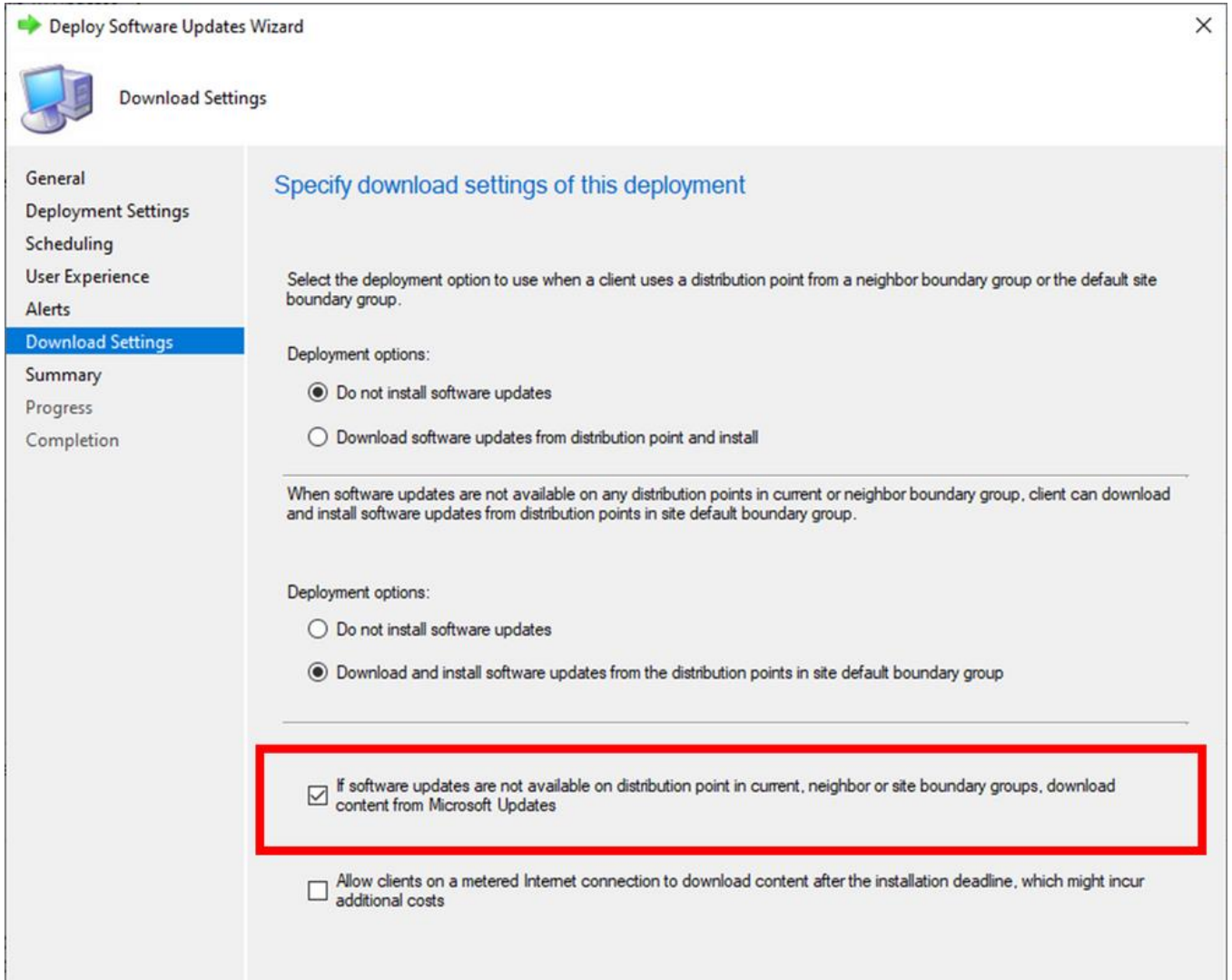




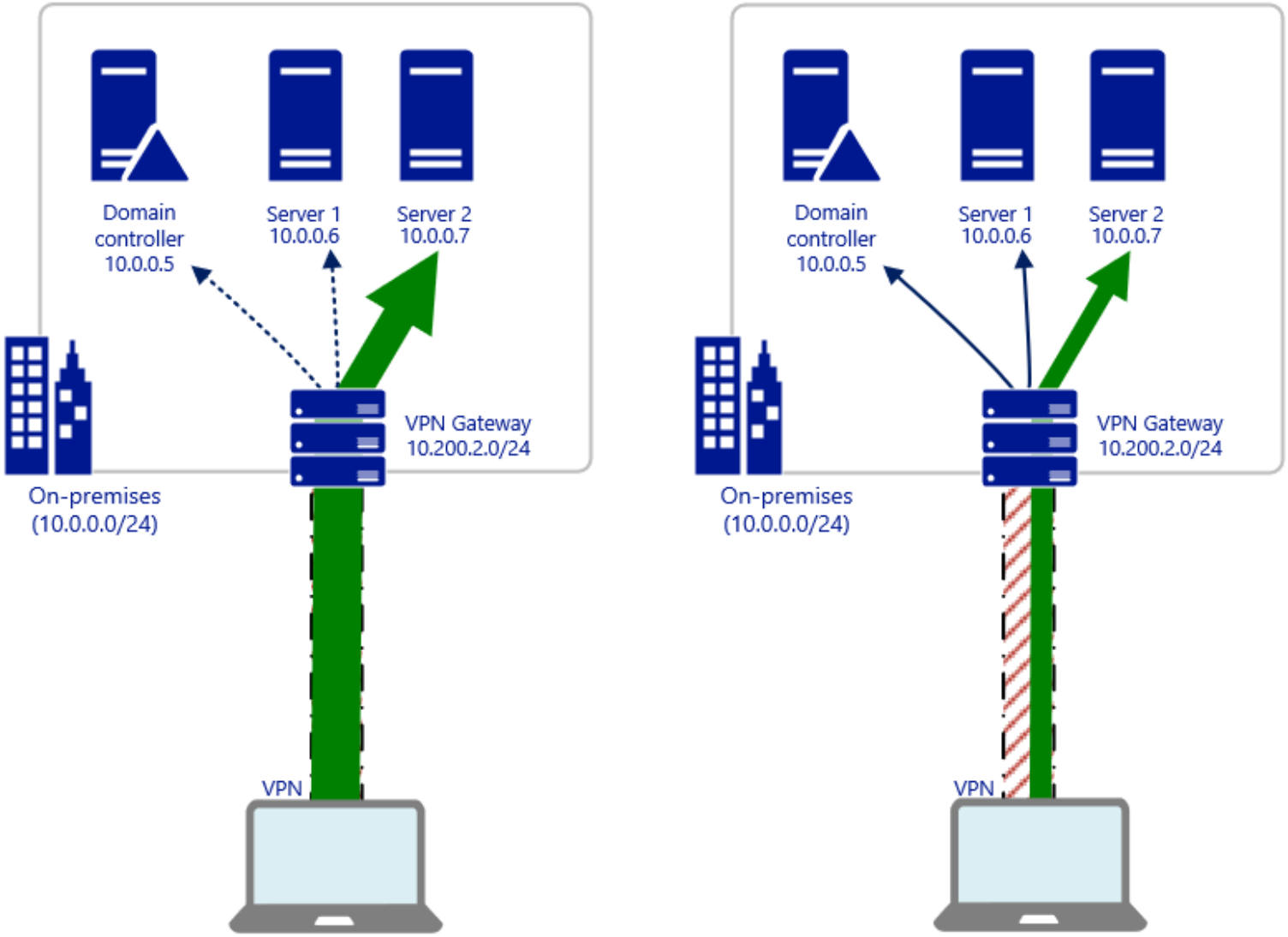
Configuration Manager

Effort
Time





VPN Bandwidth Management



https://techcommunity.microsoft.com/t5/premier-field-engineering/mastering-configuration-manager-bandwidth-limitations-for-vpn/ba-p/1280002

Domain exceptions



For Windows Update and split-tunnel which URLs have to be configured?

https://*.prod.do.dsp.mp.microsoft.com
http://emdl.ws.microsoft.com
http://*.dl.delivery.mp.microsoft.com
http://windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com
https://*.windowsupdate.microsoft.com
http://*.windowsupdate.com
https://*.delivery.mp.microsoft.com
https://*.update.microsoft.com
http://*.update.microsoft.com
https://tsfe.trafficshaping.dsp.mp.microsoft.com
http://download.microsoft.com
http://wustat.windows.com
http://ntservicepack.microsoft.com

Manage connection endpoints for Windows 10 Enterprise

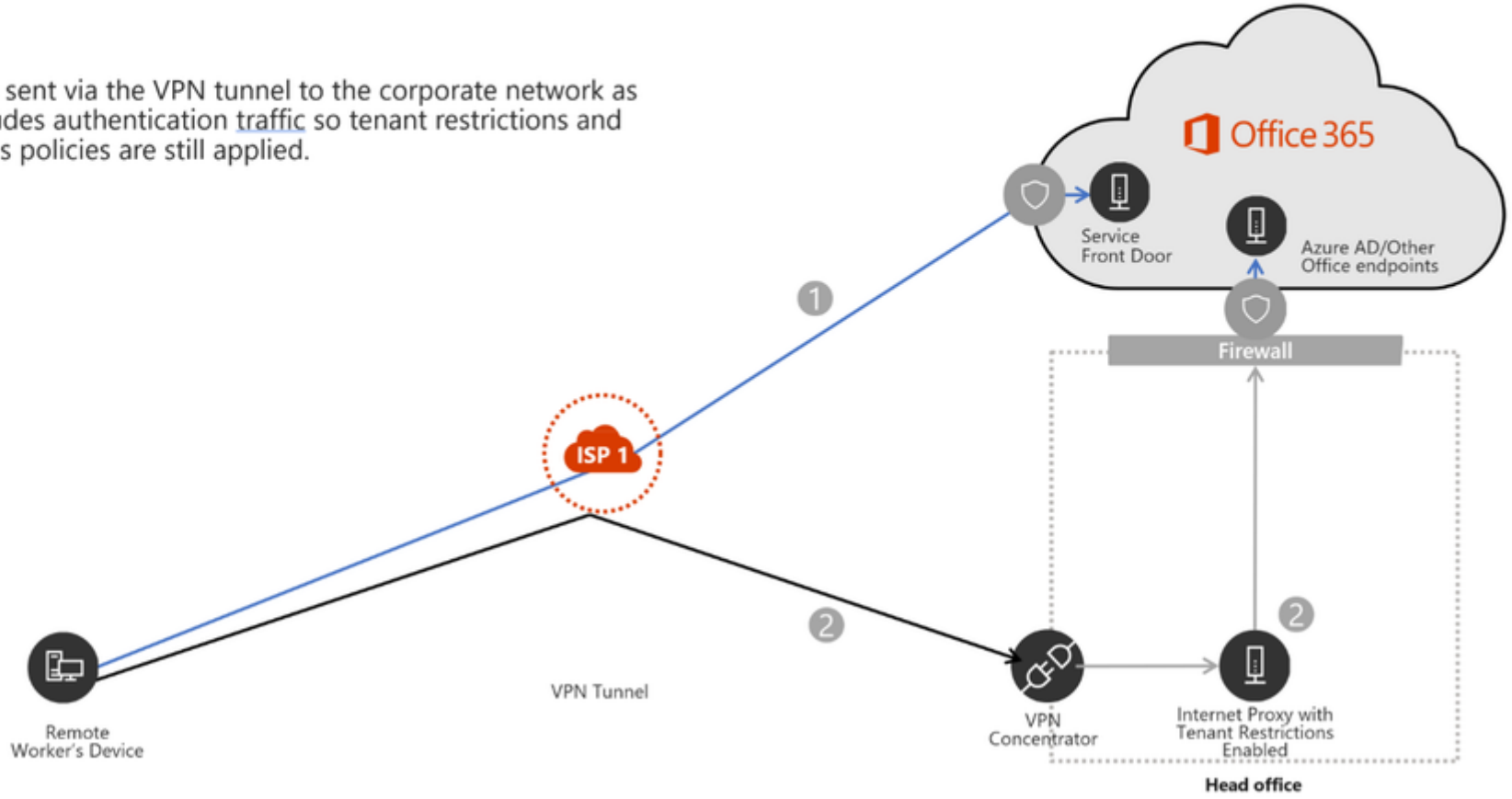
Microsoft Public IP Space

Optimize Office 365 traffic for remote staff

Split Tunnel VPN solution

1. Optimize marked Office 365 traffic is sent direct to the service via the user's local internet connection courtesy of a split tunnel policy on the VPN client

2. All other traffic is sent via the VPN tunnel to the corporate network as normal. This includes authentication traffic so tenant restrictions and conditional access policies are still applied.



https://techcommunity.microsoft.com/t5/office-365-blog/how-to-quickly-optimize-office-365-traffic-for-remote-staff-amp/ba-p/1214571

Microsoft

Questions?

Send email: artsin@microsoft.com
or text me: @ArtyomSinitsyn



Artyom Sinitsyn CISSP | MCSE | MCITP
Security Program Manager, CEE & CIS
Twitter: aka.ms/artsin

© Copyright Microsoft Corporation. All rights reserved.

What are we going to do tomorrow, Brain?



Additional information - ConfigMgr

Part 1: Helping businesses rapidly set up to work securely from personal PCs and mobiles

Part 2: Helping IT send and provision business PCs at home to work securely during COVID-19

Part 3: Manage work devices at home during Covid-19 using Configuration Manager

Part 4: Managing remote machines with cloud management gateway (CMG)

Part 5: Managing Patch Tuesday with Configuration Manager in a remote work world

Part 6: Mastering Configuration Manager Bandwidth limitations for VPN connected Clients

Additional information – Office 365

[How to quickly optimize Office 365 traffic for remote staff & reduce the load on your infrastructure]

[Implementing VPN split tunnelling for Office 365]

Additional information - VPN

Example Microsoft IT (MSIT)

14th April update will fix internet connectivity issues on devices with manual or auto-configured proxies including VPNs: Windows Message Center

VPN Performance:

https://www.microsoft.com/en-us/itshowcase/enhancing-remote-access-in-windows-10-with-an-automatic-vpn-profile

Bandwidth management:

https://techcommunity.microsoft.com/t5/premier-field-engineering/mastering-configuration-manager-bandwidth-limitations-for-vpn/ba-p/1280002#

Microsoft recommendations to work remotely with Azure and VPN:

Working remotely using Azure networking services

Remote work using Azure VPN Gateway Point-to-site

Thanks for watching

Subscribe: @ArtyomSinitsyn | YouTube





© Copyright Microsoft Corporation. All rights reserved.