How to use Citrix to prevent all browser-borne malware

This article shows how you can use Citrix XenApp and Citrix XenDesktop to isolate employees' Internet browsing, to protect against any malware or ransomware cyber attack on enterprise organizations.

By:
Ton de Vreede a Citrix Certified Professional – Virtualization (CCP – V)
Pavel Klushin a Citrix Certified Professional – Mobility

Introduction

The internet. Can't live without it, but from an IT perspective, they'd rather...

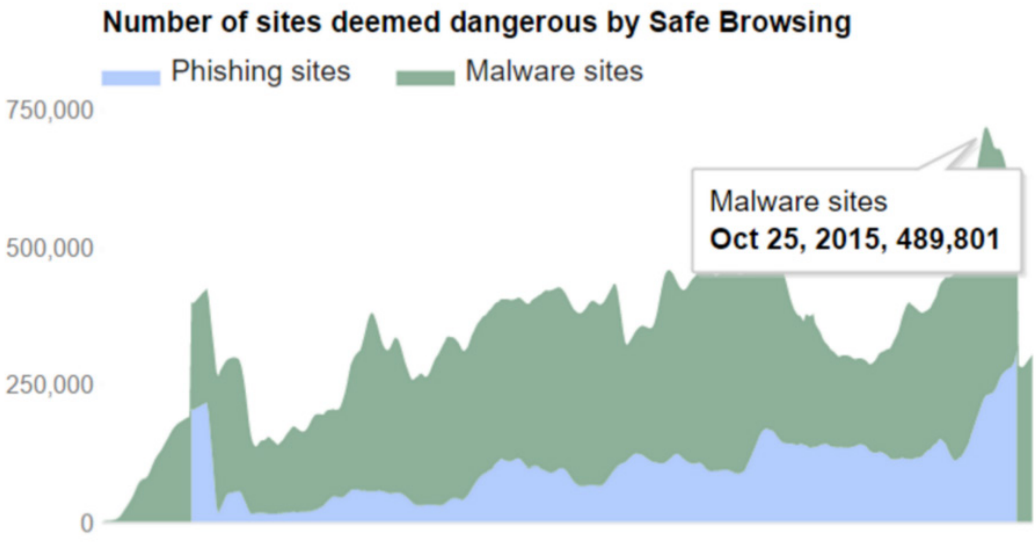
These days it's rare to find corporations and institutions that don't need their users to have Internet access. It is used to access information, applications and banking, for health and pleasure and sometimes just for watching Russian dashcam videos on YouTube. But this presents a problem. Every day more malware is written, a lot of which use new exploits that (security) software manufacturers are not yet aware of.

The continuous cycle of patching new holes in your systems, testing and deploying is a never-ending story. Your systems are up to date, you use all the required security layers and yet your IT environment will never be 100% secure unless everything is turned off. "The only secure computer is the one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location ... and I'm not even too sure about that one," said Dennis Hughes of the FBI.
So what measures can you take to reduce these risks?

Firewalling, content scanning, virus scanners, intrusion detection and URL safe lists are all methods employed to prevent malware infections of your internal network. They are effective but do not guarantee 100% security.

It's a thick layer of protection that will probably block most, but not all, malware attacks through browsing. The amount of malware out there is huge, with new variations appearing on a daily basis. It's new malware that's most dangerous, as it has not been included in the databases of security products yet.

The threat is real: 12month growth



Source: https://www.google.com/transparencyreport/safebrowsing/?hl=en

This is just what Google has detected and marked as unsafe. But even Google doesn't know everything.
Most of the detected websites probably host 'old' malware – that's how Google knows they are infected. However, just like many security products, Google can have a hard time detecting new variations of malware. There are unsafe sites Google doesn't know about while a lot of malware already has updating capabilities. The moment a new piece of malware is released hackers will push it out to the websites they 'own'.

SANS (the leading organization in computer security training) discusses malware protection and incident response in a single paragraph, indicating they understand that it is only a matter of time until malware affects corporate users, and that no-one is able to escape current sophisticated malware attacks. It seems that the old security track of thought went bankrupt and new and creative thinking should be adopted on how to deal with the most common security challenges.

How are your users browsing the Internet?

If you have a Citrix XenApp/XenDesktop environment, there are three common ways you can allow your users to access the Internet.

Browsing through the internal Citrix environment

We estimate that 40–50% of Citrix environments use this option. Using Citrix features such as HDX protocol reduces the negative impact on the Citrix environment performance, leading to better user experience than before this technology became available.

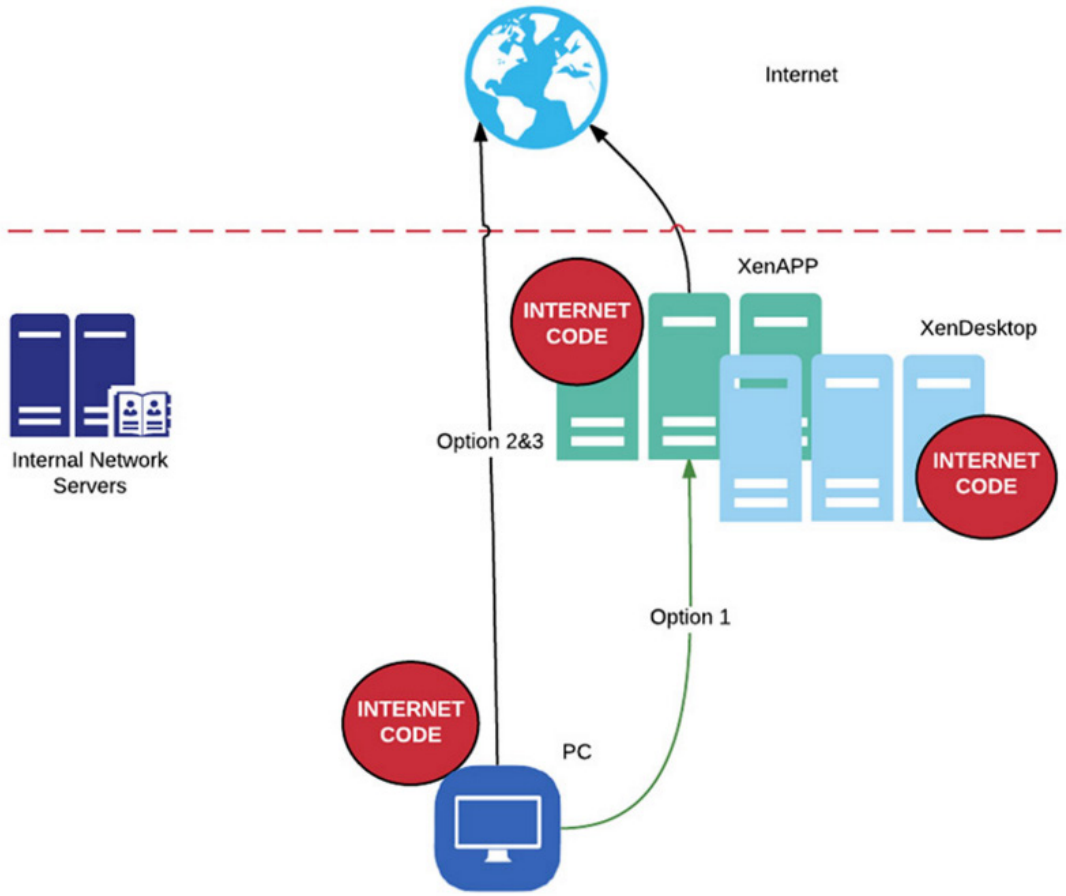
PROS

- The most transparent option for the user.
- Centralized management of your browsing security.
- If your users have different client types, there is still only one location (and operating system) where security-related browsing is managed.
- The centralized Citrix environment can be firewalled for extra protection of your internal network.

CONS

•HDX is very good. Nevertheless, browsing applications will still impact server performance, and business applications may suffer as a result of a World Cup video stream.

•Firewalled or not, if a server is compromised it might affect all the users on that server, not just the individual user on a desktop machine. In addition, the server is located inside the data center, so the Citrix environment also has access to your main business applications inside your network, which can now be compromised as a result of a malware attack.



Browsing from the user's workstation

Browsing locally on the endpoint can make sense, especially if Citrix seamless applications are used instead of full published desktops:

PROS

- With a capable machine and network, this will provide your user with the best performance.
- Your Citrix environment will not suffer a browsing-induced performance impact.
- If your LAN is segmented properly, malware infections may be contained to a small part of your LAN and not more widely in the data center.

CONS

- Decentralized management often means longer implementation timeframes for security updates and changes.
- If your endpoints are several flavors of Windows, some Macs and the occasional Linux machine, you will need to secure these machines with several different technologies. This is time consuming, requires more in-depth knowledge of several operating systems and thus opens up the potential for errors in your configuration.
- The attack surface in this model is bigger as there are more endpoints to protect in comparison with a centralized system, and network traffic is distributed through the corporate network instead of being limited to a specific area in your server network.
- Your users probably have one account for both the desktop and Citrix environment. If this account is compromised hackers can still gain access to your internal business applications.
- A user's "workstation" is often a laptop. As most users take it home, the security threat grows immensely because you don't have control over their network traffic.

'Internet only' dedicated workstations

This is potentially the most secure option. If secured properly, workstations that are only allowed to access the Internet and nothing else on the network can limit any malware infections to a single machine. All the more so if these machines are physically separated (as much as is possible in a network environment) from the rest of the LAN.

PROS

- Malware infections are limited only to machines that have access to the Internet, and nothing else.

- You can choose the operating system for the machines you are most comfortable securing. Consequently, patching and securing will be less work because there is only one “machine flavor”.
- In most cases, these machines do not store persistent user data. Consequently, it is easy to restore a machine with a default image if it has been compromised.

CONS

- Unless you plan on providing each user with their own extra workstation, there will always be a time when several users need to access the Internet and have to wait. Or somebody walks away from the machine for a minute, another user logs off the previous user and work in progress is lost.
- NO integration with your business environment. Hello Mr USB Drive. Hello Mr Malware On USB Drive.
- One machine is not a problem, but when you want to provide these workstations for several departments extra desk space and infrastructure will start to add up.
- Having to go to a different workstation than your own every time you need something from the Internet is simply a pain and will harm business productivity.
- In most cases you would still have to allow some external Internet connections from the LAN environment for email communications, SaaS applications, etc.

The challenges

Top organization users secure browsing challenges:

- Establishing a secure browsing farm with optimal user experience, based on XenApp/ XenDesktop.
  - Browsing farm sizing
  - Browsing farm hardening (both browser and server)
  - Transparent user experience (retaining cookies, favorites, history etc.)
  - Flash blocker for maximum performance and security (not always possible)
  - EnablIng file downloads and delivery
  - Monitoring and optimization of corporate browsing activity
  - Enabling anonymous corporate browsing to prevent user information leak SSO (Single Sign On) support
- Safe browsing of any website.
- Compliance with local regulatory requirements.
- Minimal effort required to implement the organization’s browsing policy.
- As transparent/easy to use for the end user as possible.

Citrix Secure Browsing solution brief

To set up a DMZ Citrix Internet browsing farm for browsing outside your corporate network, a number of corporate organizations realized that the ultimate way to defeat malware was to isolate Internet browsing. Consequently, these organizations built a separate XenApp /XenDesktop environment on their DMZ in order to access the Internet safely.

This way, all external content is executed outside the corporate network so that malicious code can't run internally. The only traffic entering your network from the DMZ is screen updates, prints or clipboard items. The last two can be disabled or configured to lower the risk of harmful content which may harm internal desktops, cause data breaches of the desktop, internal applications, databases and sensitive data.

By isolating browsing traffic in a Citrix environment in the DMZ you get the best of both worlds:

- A centralized environment is the easiest to secure and manage.

- Separation: Any malware infection can be contained to the DMZ, where your core business applications are not hosted.

- You can go to extremes in firewalling this Citrix environment as the only ports needed are the standard Microsoft and Citrix ports, and port 80 and 443 for Internet browsing.

- A lot of browser functionality that is required for your core business applications, such as running scripts, isn't required for browsing the Internet. Yes, some websites may have issues but you can still use some more relaxed settings for these if they are required for the business. Your default setting can be more secure.

- Browsing traffic will be offloaded from your internal Citrix farm. It will still be a load on your environment as a whole but the chances of disruption to your business activities will be reduced. Kim Kardashian may break the Internet but your internal environment will perform as usual.

- The risk in continually patching your system with the latest security updates is that they could break one of your core applications. The odds of a security update breaking a system that only runs a browser and not much else are much lower. Before you deploy the required updates in your environment, use the DMZ farm to test the updates. Once you know how it affects your core applications, you can patch your Internet farm almost straight away,. You already know how to do most of this. It's just like your internal Citrix environment, only simpler as you will not need the myriad of applications that you need to run your business.

There are also some cons

There is extra management of this farm. And you will need more computing power to run an additional one. However, user browser performance shouldn't be affected because your DMZ will often be in the same physical location as your internal network. If you use a full published desktop you can set up content redirection to launch ICA files on your endpoint. You will simply be connecting to two farms simultaneously so the internal farm stays completely out of the picture. Also, users will need to launch a separate browser (the Citrix published application) for accessing the Internet.

Some internal applications will need access to the Internet.

Just set up some firewalling and allow them. Again, the default can now be to not allow any traffic and just open up what's really necessary.

'I run some core business applications on the Internet'

You can easily set up an extra delivery and published applications group for these applications. The only difference from your 'standard' browsing servers will be the allowed site list (or blocking through proxy, whichever you prefer). You will isolate your Internet browsing to a lesser degree as it is in the same farm as these applications but still much safer than browsing the Internet from inside your internal network.

Isolation? Well worth it!

Isolation is the keyword here. Mixing internal and external browsing in the same environment is a security challenge. This is because malware downloaded by mistake from the Internet can easily cause an internal data breach. By isolating your external browsing traffic to your DMZ this will no longer be a problem.

How to build this solution

In order to build a secure, Citrix-based browsing farm on your DMZ environment you must have StoreFront servers to access your browsers, and Citrix controllers to manage your browsing farm. It is highly recommended to use the following components in order to get optimal performance and the highest level of security for the solution.

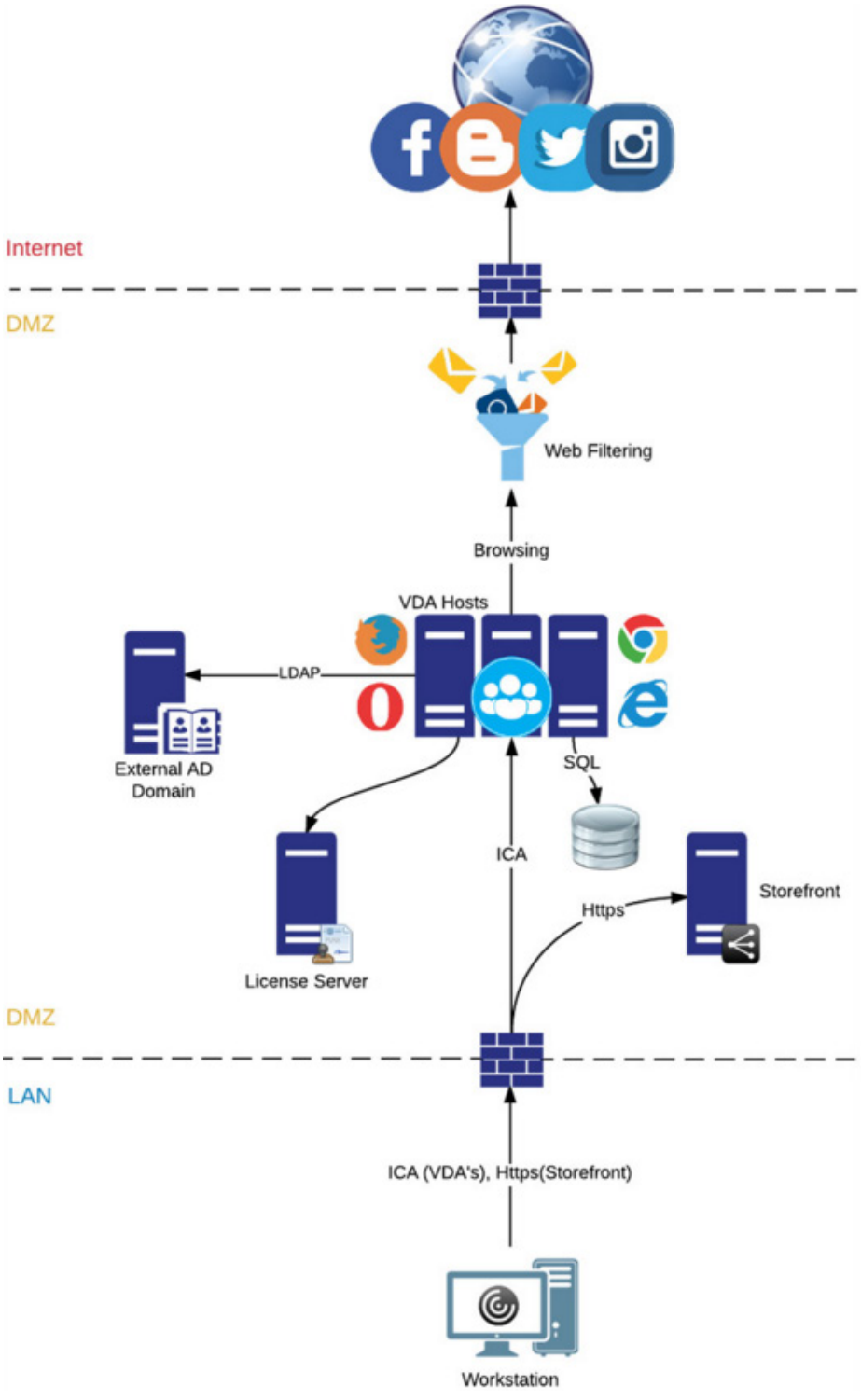
Solution Components

Elements needed	Function
SQL Server	Database of XenApp farm. This component acts as a central repository for all static information existing on the farm, including data such as users, policies and a list

	of servers and applications distributed on the farm. Each XenApp server controller has an open session in front of the Data Store. Note that this SQL server only contains the databases required for Citrix. No sensitive corporate data is stored here.
XA Controller	A software component installed on a Windows server. This software distributes and manages a list of applications and servers. It also enforces application policy.
StoreFront	Citrix StoreFront is an enterprise app store that will publish the corporate XenApp browser.
License Server	A software component installed on Windows servers. The license server stores the licenses and manages the Citrix license usage in real time.
Image provisioning solution	Eliminates the need to configure each server individually, by defining a single server and replicating it to a large number of servers joining the farm using Citrix technology Provisioning Services (PVS). If the server is rebooted, it reverts to a "clean" state without any damage or changes.
Citrix Receiver	Software components installed on end-user workstations. The Citrix Receiver allows direct connection through the HDX protocol from the edge of the XenApp servers. The Citrix Receiver is supported in a variety of terminal equipment such as Windows workstations, thin clients and smartphones.
Active Directory	Implementation of external Microsoft-based Active Directory (AD) to build a new entity for every user that browses the Internet. This AD should be an independent entity, only storing information for the Internet browsing environment.
Storage Space	For the roaming profiles.
Citrix User Profile Management	Profile management ensures that the user's personal settings are applied to the user's virtual desktop and applications, regardless of the location and endpoint device.

Solution diagram

CIGLOO

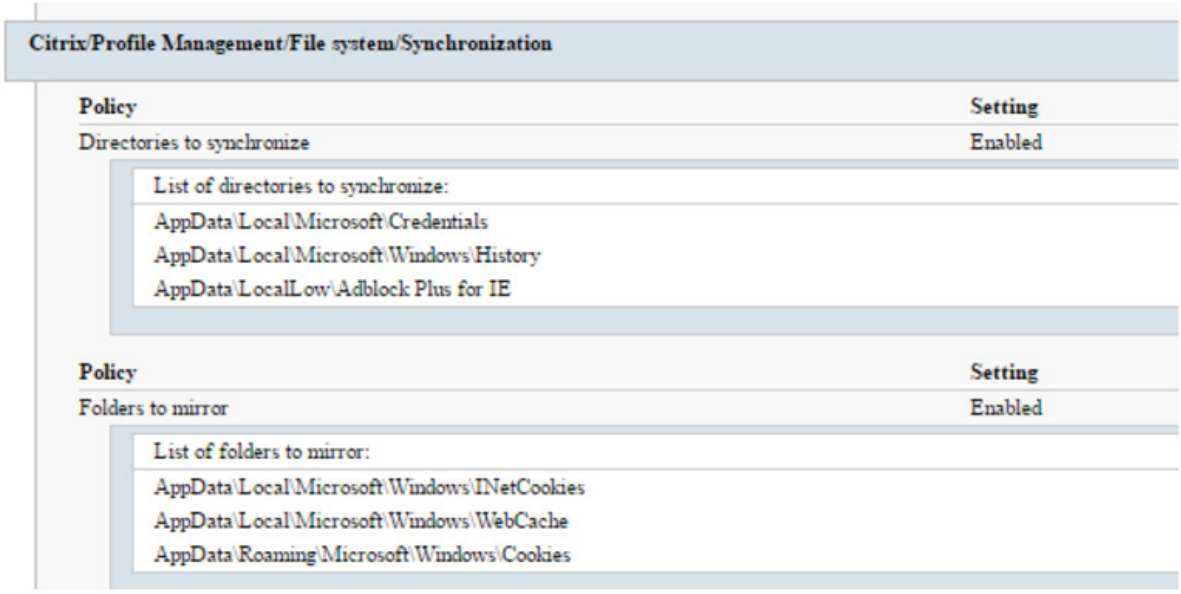


User environment configuration

In order to achieve great user experience we must consider a few key components:

1. Saving user cookies and passwords – users don't like to enter their credentials each time they access their accounts
2. Saving user favorites
3. Saving user history
4. Configuring ad blocker – blocking flash banners and popups will reduce the annoying ads and help increase server performance

The best and easiest way to configure these is by using **Citrix User Profile Manager Version 5.X.** At the Citrix UPM GPO we need to configure the following to preserve user cookies, history and favorites:



Citrix/Profile Management/File system/Synchronization	
Policy	**Setting**
Directories to synchronize	Enabled
List of directories to synchronize:	
AppData\Local\Microsoft\Credentials	
AppData\Local\Microsoft\Windows\History	
AppData\LocalLow\Adblock Plus for IE	
Policy	**Setting**
Folders to mirror	Enabled
List of folders to mirror:	
AppData\Local\Microsoft\Windows\INetCookies	
AppData\Local\Microsoft\Windows\WebCache	
AppData\Roaming\Microsoft\Windows\Cookies	

Saving "favorites" for user profiles is done by creating a folder redirection policy for the Favorites folder.
We recommend installing ABP as your ad blocker.
The best way to deploy ABP in a Citrix XenApp environment is by following these steps:

1. Install ABP from https://adblockplus.org/ on your Gold Image server or, if you are not using PVS/MCS systems, on all XenApp servers.
2. Configure a policy that will enforce use of this extension to all users:
In **User Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Security Features/Add-on Management/Add-on** List, enable policy and configure with these values:
Value name: {FFCB3198-32F3-4E8B-9539-4324694ED664}
Value: 1

* Note that some sites are aware of this extension and can send a popup message to users, such as "Please turn off the ABP blocker in order to proceed using this web site".

There is a manageable exclusion list that is located in every user profile: c:\users\%username%\appdata\locallow\Adblock Plus for IE\patterns.ini

To add a domain/site to be excluded from AdBlock:

1. Open patterns.ini in notepad++
2. Scroll to the very bottom. Add this code:
Code: Select all
[Subscription filters]
@@||domain.com^$document
Replace “domain.com” with the domain of the site you wish to whitelist.
3. Then create a GPP to enforce this file for all users:
Under User Configuration > Preferences > Windows Settings > Files, create a new file action. Set the action type to “Replace”.
4. Set source file to the network path location of the patterns.ini file. Under destination, enter the path exactly as c:\users\%username%\appdata\locallow\Adblock Plus for IE\patterns.ini.
5. Click on the “Common” tab and check the box for setting “Run in logged-on user’s security context”. Then click OK.
**You can download the full user environment and server hardening GPO – please contact us at www.cigloo.io

System Environment

Restart policy

Citrix best practice highly recommends to restart XenApp servers once a week in order to free all the unnecessary processes still allocated in the memory. We recommend restarting the servers once a day to keep the environment safe from any changes.

Performance
We highly recommend using PVS as the provisioning system and to configure the Vdisk with “RAM cache with overflow to hard disk”. This option will give your server file access speeds comparable to or better than SSDs.

Users and XenApp server sizing

Sizing your browsing farm with Citrix infrastructure

Browsing is probably the most variable process in terms of compute resource use that an environment has. You could have dozens of users on a simple website using relatively little resources, but if one user goes to a multimedia, content-heavy website they could suddenly be using a full CPU core and a lot of memory. The good news is you will be removing this unpredictable load from your internal environment

(the load of your internal web applications won't vary much).

As a starting point, get an overview of the current amount of CPU, memory and perhaps disk I/O being used (this is easy using tools like ControlUp). Then estimate how much of this computing resource you will be offloading to the browsing farm, and calculate what is needed.

Remember this is just a starting point. Browsing resource use is difficult to calculate or benchmark. There is no substitute for live testing. Consider moving your users to the browsing farm in small groups instead of a 'big bang' migration so you can get a feel for the resources required.

In our experience, a Windows 2012 R2 server with 4vCPUs and 24GB RAM will support about 40 users (using latest hardware and not over provisioning physical servers). For example, say an organization has 1,000 corporate users browsing external URLs. The estimation depends, of course, on the organization's browsing behaviour but basically you can estimate a ratio of 1 concurrent user for every 2.5 named users.
Hence, for 1,000 users you can estimate about 400 concurrent users. Every XenApp /XenDesktop server supports up to 30 concurrent users,. So, in this example, the organization will need 13–14 virtual servers in order to create the browsing farm.

Activity monitoring

In addition to your usual monitoring of farm performance, consider logging the websites that users visit as well. Citrix Director cannot do this but there are 3rd-party applications like ControlUP that can. They will also generate extensive reports such as what are the most visited websites at certain times.
Take your local privacy laws into consideration when setting up URL logging. Anonymous logging for statistical purposes is usually not a problem, but recording each website a specific user visits may be.

Domain security

It is highly recommended to create a separate domain for the Citrix servers in the DMZ to achieve maximum protection of the identity of your internal LAN users.
Also, you can create a different account name for the DMZ domain users (maybe some random numbers) so their corporate identity can't be stolen when they are using the Internet.

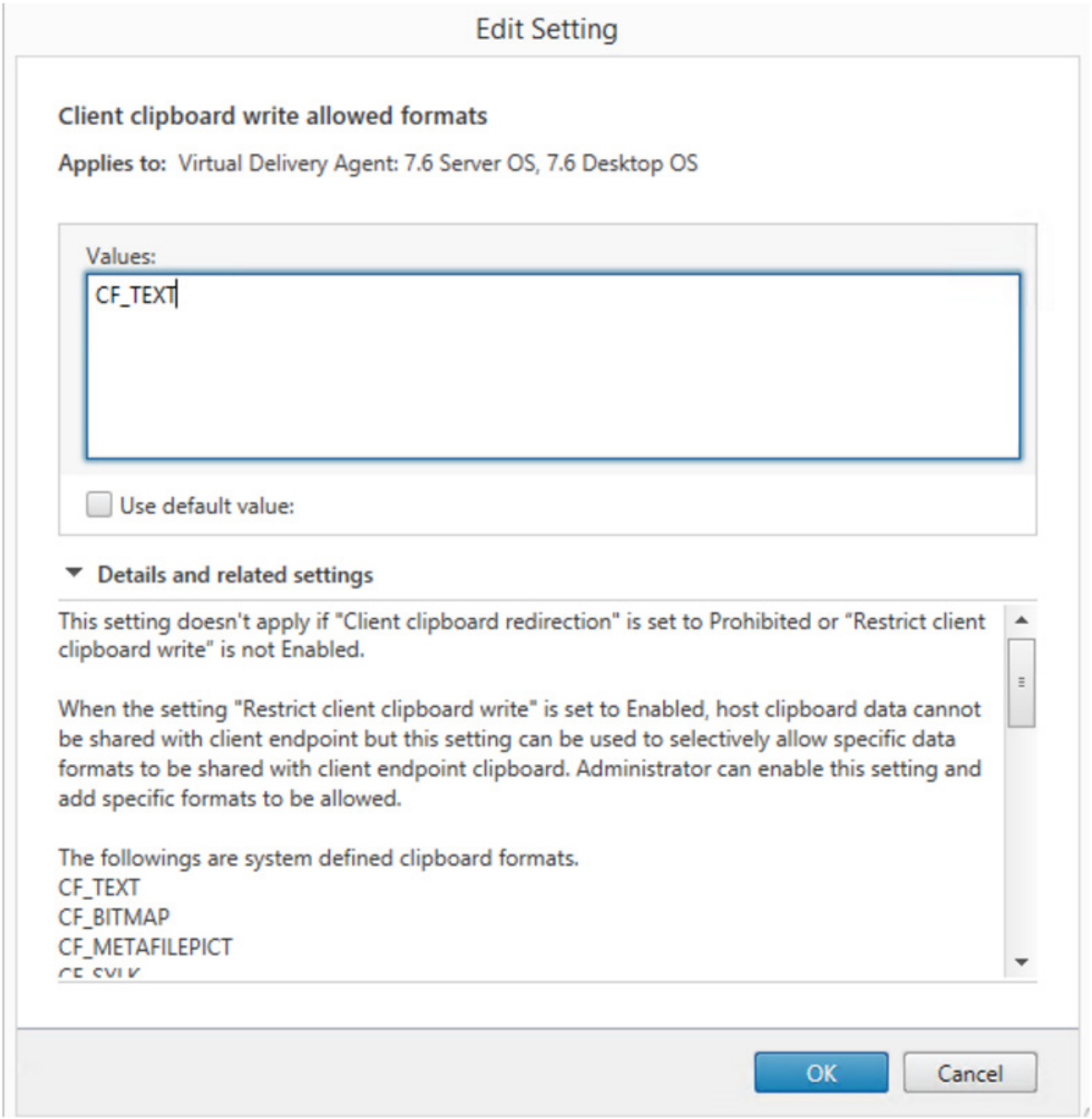
Web browser published application

The most important procedure is publishing the web browser to the users.
When using Windows 2012 R2 servers, keep in mind your default web browser is IE 11 and that there are still some sites that don't support IE 11, Chrome or Firefox. If you require support of old browsers such IE 8/9 you will need to create a dedicated Delivery Group with Windows 2008 R2 servers and old browsers.
There is no automatic method, with Citrix or Microsoft systems, for redirecting

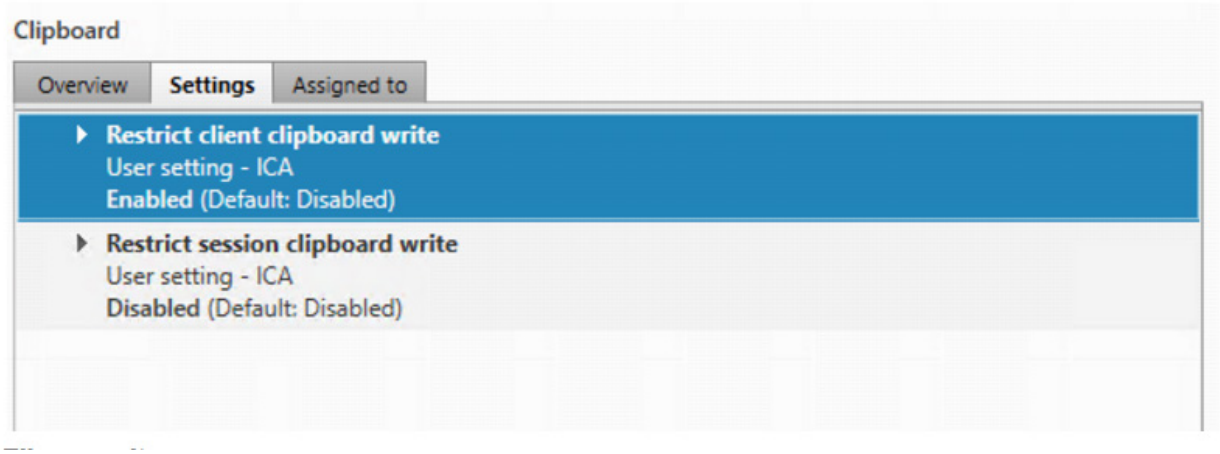
users to different sites by using different web browsers without using 3rd-party applications. The administrator will need to publish all the web browsers with predefined URLs for the old websites (or to educate users to use the “IE7” published icon to open the old sites that they need to access).

Clipboard management

We aim to harden browsers and servers as well as the ICA protocol so the session is highly secured.
Using Citrix Policy for client clipboards allows you to harden the protocol so it copies only certain formats. It is recommended to allow copying in text format only. In most cases users will receive some long URL which is convenient to copy and paste. Using this policy lets the administrator ensure that only text is copied while any other format, malicious code included, can’t enter the ICA session.



Another hardening policy to consider is denying users the ability to copy from the XenApp session into their endpoints, but allowing them to do so from the client to the session.



File security

As best practice for securing XenApp servers it is recommended to install some kind of an anti-virus (AV)system designated for handling malware. When installing AV software on XenApp servers don't forget to make a unique policy for excluding unneeded folders and system process on the servers as advised by Citrix.
It is also recommended to use a URL filtering system to protect your system from downloads of untrusted files or accessing URLs that are designated as unsecure sites. Therefore we recommend using 3rd-party web security gateways such as Blue Coat and Websense.
Browser hardening (GPO) – in order to keep the browsing environment safe we must harden it at every level.

Citrix HDX

HDX can be used to take a lot of the strain off displaying multimedia away from your browsing farm. Use it wisely to redirect certain media to your endpoints and have it rendered there instead of on the server. If a server has to render multimedia content it won't use a lot of CPU for that. However, it will also have to encode the stream back into ICA for display on the endpoint.

A complete guide to setting up HDX goes beyond the scope of this article (and if you use Citrix this has most likely been investigated by your Citrix administrators anyway) but here are some useful links:

White Paper: HDX technologies for optimizing application and desktop delivery
ICA Policy Settings: Multimedia
A bit older but still useful: HDX Troubleshooting Guide

For best performance, consider equipping your servers with some (Nvidia) GPUs. These are used for transcoding multimedia and will reduce the strain on your general-purpose CPUs considerably.

DO's and DON'Ts

DO's

1. Use read-only server images, and reboot them daily to make sure they stay clean.
2. Keep your user profiles clean and small. In many cases it is sufficient to store just the browsing history, favorites/bookmarks and cookies of the users on the browsing farm.
3. Remember to set up HDX and content redirection where required.
4. Run a sizing test before going live with the system. Your users may be accessing vastly different websites from the ones you did a quick performance check on.
5. Make the appearance of the 'Internet browser' sufficiently different from the normal browser to allow users to see quickly where they can go in that browser. For example, In Internet Explorer it is quite easy to change the color of the title bar to bright red by changing the Windows color scheme.
6. Create an external domain so as to not expose your corporate user accounts on the Internet.

DON'Ts

1. Don't forget about hardening – even though your servers are now isolated in the DMZ. A security breach may be less of a problem but it still is a problem.
2. Don't blindly redirect everything to your endpoints with HDX. Media content can also be a risk. If you do decide to allow Flash (sometimes a necessary evil), set up a Flash whitelist to only allow sites where it is really needed.
3. Don't tell your users that browsing the Internet will be exactly the same as before. They will have to use a separate browser for Internet browsing. It does not have to be a big deal but you do not want to be burned at the stake for making promises you can't deliver. Instead, explain to users why this is the way to go. It can't hurt to remind them that it is not only the company's environment that is at risk but their personal data as well.