REVISED 10 SEPTEMBER 2018

BLAST EXTREME DISPLAY PROTOCOL IN VMWARE HORIZON 7

Horizon 7 version 7.5 and later

vmware

Table of Contents

Blast Extreme Display Protocol in VMware Horizon 7

Introduction

Blast Extreme is included with the View component of VMware Horizon® 7, the latest generation of VMware desktop virtualization and remote application-delivery software.

Blast Extreme represents an evolution of the display protocol used for VMware Horizon® HTML Access™. Blast—the name of the first version of the protocol—started as a TCP-based protocol. It used a JPG/PNG-based codec to deliver desktops to a browser rather than requiring a native VMware Horizon® Client™ on each endpoint device. With Horizon 7, Blast Extreme brings Blast into feature parity with the PCoIP display protocol. Blast Extreme is used for HTML Access and can be used for native Horizon Clients (version 4.0 and later).

Blast Extreme can also use the H.264 codec as well as the JPG/PNG codec and automatically selects the most suitable codec for the conditions. The H.264 codec gives performance and experience benefits. With H.264, the protocol can be encoded on the server using either hardware or software processing and decoded on the local endpoint using either hardware or software (hardware is the default unless the client is not H.264-capable). Servers fitted with NVIDIA GRID graphics acceleration cards can offload H.264 encoding to the hardware in the NVIDIA GRID card.

This guide provides a technical description of Blast Extreme, including how to deploy it, configuration best practices, and benefits and limitations, for administrators who are considering using the Blast Extreme display protocol in their organization today.

Use Cases

VMware recommends Blast Extreme for most use cases. It is required for connections to Linux desktops and for HTML Access. HTML Access uses the JPG/PNG codec except for Chrome browsers, which can be configured to use the H.264 codec. For a detailed description of these codecs, see Codecs Used by Blast Extreme.

The only end users who should continue to use PCoIP rather than Blast Extreme are users of zero-client devices that are specifically manufactured to support PCoIP. For a list of zero and thin clients that support Blast Extreme, see the VMware Compatibility Guide.

Note: If you configure a pool to use Blast Extreme and do not allow users to choose a protocol, the Connection Server automatically allows PCoIP connections from PCoIP zero clients and older (pre-4.0) Horizon Clients.

When used in an NVIDIA GRID vGPU solution, Blast Extreme outperforms PCoIP for 3D rendering in graphics-intensive applications, and it can enable hardware encoding in addition to hardware decoding. For a performance comparison of PCoIP and Blast Extreme, see the blog post VMware Horizon Blast Extreme Acceleration with NVIDIA GRID.

Blast Extreme Benefits

Blast Extreme provides

- Broad client support, including Windows, Linux, Mac, Android, iOS, Chrome, and web (HTML Access) clients.
- Ability to meet performance requirements for visually intensive applications when used with NVIDIA GRID GPU–based hardware acceleration in the host.
- Significant improvements in bandwidth and performance optimization with Horizon 7 version 7.1 and later (and Horizon Client 4.4 and later), using Blast Extreme Adaptive Transport.
- Ability to use either the TCP or the UDP network transport. PCoIP uses only UDP.
- Intelligence to determine network conditions. In clients prior to Horizon Client 4.8, users were required to choose from three options to describe their network conditions, namely "Excellent," "Typical," and "Poor." With Horizon Client 4.8, these three options have been removed from all native clients except Horizon Client for Windows 10 UWP. The Blast Extreme networking stack now dynamically chooses the right mode. This built-in intelligence is called Blast Extreme Network Intelligent Transport (BENIT). See the BENIT FAQ section.
- Lower CPU consumption for longer battery life on mobile devices when the H.264 option is turned on. H.264 allows the device hardware to perform video decoding.

- Feature parity with the PCoIP display protocol, including multiple-monitor support for up to four monitors (requires Horizon 7 version 7.1 and Horizon Client 4.4 if using the H.264 codec).
- Simple management with Windows Group Policy or Horizon 7 Smart Policies included with VMware User Environment Manager™ 9.1 or later.
- Option to simplify setup, including opening only one port (TCP 443) on front-end firewalls when VMware Unified Access Gateway™ is used as the secure gateway.

Evolution of Blast Extreme

VMware has used the Blast display protocol in some form since March 2013, when the first version of HTML Access was released with View 5.2. HTML Access allows users to connect to virtual desktops and published applications from HTML 5–compliant web browsers without the need for Horizon Client software on their client systems.

For example, users can use HTML Access

- On devices for which there is no native Horizon Client
- On computers that the user does not own
- On computers for which the user does not have the administrator privileges required to install Horizon Client

An early version of Blast was also used for Horizon 6 for Linux, first released as part of Horizon 6 version 6.1.1, in June 2015. As with HTML Access, Horizon 6 for Linux and Horizon for Linux versions 7.0–7.0.2 use only the JPEG/PNG codec and use only TCP.

The Blast Extreme display protocol was released with Horizon 7. To see all of its features, you must use Horizon Client 4.0 or later, which was released at the same time as Horizon 7 version 7.0. The following table summarizes the differences in Blast Extreme capabilities when used with various clients and desktops.

	HORIZON CLIENT 4.0 OR LATER	HTML ACCESS 4.0 OR LATER	HORIZON FOR LINUX
TCP	Yes	Yes	Yes
UDP	Yes	No	7.5 or later
JPG/PNG codec	Yes	Yes	Yes
H.264 codec	Yes	Chrome 45 and later	7.0.3 or later
Hardware decoding	Yes	Chrome 45 and later	7.0.3 or later
Feature parity with PCoIP	Yes	No	7.5 or later

Table 1: Comparison of Protocol Features for Horizon Client, HTML Access, and Linux

The version of Blast Extreme used for HTML Access and for connecting to Linux virtual desktops does not have all the remote-experience features that are available for Blast Extreme with a native Horizon Client when connecting to Windows virtual desktops. Remote-experience features can include virtual printing, Windows media redirection, Real-Time Audio-Video, and other features that contribute to a rich user experience. For a list of the features available with the most recent version of HTML Access, see the VMware HTML Access documentation. For more information about features available for Linux virtual desktops, see Setting Up Horizon 7 for Linux Desktops.

Blast Extreme Technology

Blast Extreme can use the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). For H.264-enabled client devices, the default is H.264; for devices that are not capable of hardware decoding, Blast Extreme uses the JPG/PNG codec.

Blast Extreme uses lossy compression by default, but it can also be configured for lossless compression.

Lossy and Lossless Compression

Multimedia files such as audio, images, and video, are compressed to reduce their size. Smaller files require less disk space for storage and less bandwidth for transmission. The two main types of compression are *lossy* and *lossless*.

- Lossy compression is irreversible. It reduces the file size by permanently eliminating certain information, especially redundant information.
- Lossless compression, which is often used for text and data files, is reversible. When the file is uncompressed, all the original data is recovered.

Well-designed lossy compression technology is perceptually lossless. Only the least significant data is lost, and there is no degradation in perceived quality. For instance, sometimes an image is blurred in the first instant it appears, and then quickly becomes sharper. In most cases, this means that the lossy compression is building to an image that is perceptually lossless.

Some use cases, such as medical imaging and graphic design, might require that the image be built to a completely lossless state, so that when the file is uncompressed, all the original data is recovered. Regardless of the protocol, however, the ability to build to lossless works only on static data. To configure Blast Extreme for lossless compression, see Configuring Images to Build to Lossless.

UDP and TCP Transport Protocols

Both TCP and UDP transmit packets of data over the Internet. TCP is the most commonly used Internet transport protocol. It uses two forms of control to guarantee that the recipient receives error-free packets of data. TCP numbers the packets, so that if the recipient does not send a message back saying that the packets were all received, the sender resends the packets. The packets are also checked for errors.

UDP transmits datagrams, which are also packets of data, but, in contrast to TCP, UDP does not use control mechanisms for arrival, delivery time, or confirmation of receipt of packets. Because UDP does not require the overhead of communication between the sender and receiver, and because no error checking is done, the sender and recipient can communicate more quickly. UDP is used when speed is the most important consideration, such as for live broadcasts and online games.

With UDP, if a connection is interrupted for a few seconds, the video freezes for those seconds and then jumps to the current bit of the broadcast, skipping any intervening bits. If minor packet loss occurs, the video or audio might be distorted for a few seconds while the audio continues to play without the missing data.

Codecs Used by Blast Extreme

Depending on circumstances and configuration used, Blast Extreme uses either an H.264 codec or a JPG/PNG codec. A codec is a computer program that can encode or decode a digital data stream for transmission. The word codec is a blend of the words coder-decoder. By default, Blast Extreme uses the H.264 codec if the client device supports that codec.

JPG/PNG Codec

The JPG/PNG codec performs software encoding and decoding of video and images. The JPG/PNG codec supports lossless compression. JPG/PNG is referred to as the adaptive *encoder*, not to be confused with adaptive *transport*. It is the best choice for

- Images that require lossless compression
- Applications such as word processors or spreadsheets, which are composed of static content

H.264 Codec

H.264, also known as AVC (Advanced Video Coding, MPEG-4 Part 10), is a commonly used video format for the recording, compression, and distribution of video content, for example for Blu-ray discs.

With Blast Extreme, H.264 provides software encoding and hardware decoding on supported devices. Tablets and phones can perform H.264 hardware decoding, as can computers manufactured in 2013 or later.

When users use Blast Extreme on one of these devices and enable H.264 hardware decoding, the graphics processor on the device does the work involved in playing back video and images. In contrast, when users use the JPG/PNG software codec, the CPU on the device, rather than the GPU, does the work. When users use H.264 hardware decoding and thereby offload the work to the GPU, CPU consumption is reduced, resulting in less device power consumed, for longer battery life.

H.264 Codec When Used with NVIDIA GRID

VMware designed Blast Extreme in partnership with NVIDIA so that NVIDIA GRID vGPU can use H.264 to offload codec encoding as well as offloading the GPU rendering. This form of hardware-accelerated graphics rendering can be used for demanding graphical workloads, such as geographic information systems (GIS) applications used for analyzing large data sets, creating maps, and visualizing scenarios of the outside world, in both 2D and 3D.

Other benefits include the following:

- Immersive 3D graphics experience on lower-cost PCs, including Chromebooks
- Increased scalability when multiple virtual desktops share an NVIDIA GRID GPU
- Delivery of up to 4K resolution displays for workstation environments
- Reduced overall latency

For more information, including information about performance benefits, see the blog post VMware Horizon Blast Extreme Acceleration with NVIDIA GRID.

Agent-Side Components

Three Blast Extreme components are built into the Horizon Agent, which you install in virtual desktops and Microsoft RDS hosts:

- The VMware Blast service (`VMBlastS.exe`) manages user sessions, proxies incoming TCP connections, and prepares the Blast Worker process.
- The Blast Worker process (`VMBlastW.exe`) captures the screen and handles everything within the session.
- If you use UDP, the Blast Proxy process (`VMBlastP.exe`) brokers UDP connections.

Log files for all three of these components are located in the following directory:`<Drive>:\ProgramData\VMware\VMware Blast\`

- The `Blast-Service.log` file contains entries that tell you whether UDP or TCP is being used. It also indicates if Blast Extreme Adaptive Transport is being used and which port is being used. (Blast Extreme Adaptive Transport is the revised version of Blast UDP, introduced with Horizon 7 version 7.1.)
- The `Blast-Worker-SessionId<#>.txt` file contains entries that tell you whether the JPG/PNG or the H.264 codec is being used.

For more information about the entries in these log files, see Verifying Successful Configuration.

Blast Extreme Connections

The following sections describe the workflow of connections made when Blast Extreme is used with the native Horizon Client.

Note: If you use HTML Access rather than a native Horizon Client, the Blast Extreme connection made to either the Connection Server or the Unified Access Gateway server is on TCP port 8443. The connection then made from the Connection Server or Unified Access Gateway to the agent in the virtual desktop or RDS host is on TCP port 22443. USB redirection, multimedia redirection (MMR), and client-drive redirection (CDR) are not available for HTML Access.

Internal Connection

With an internal connection, the client, the server, and the virtual desktop or RDS host are all inside the corporate network. The following diagram shows the ports used for an internal connection, and the list that follows describes the order in which the connections are made.

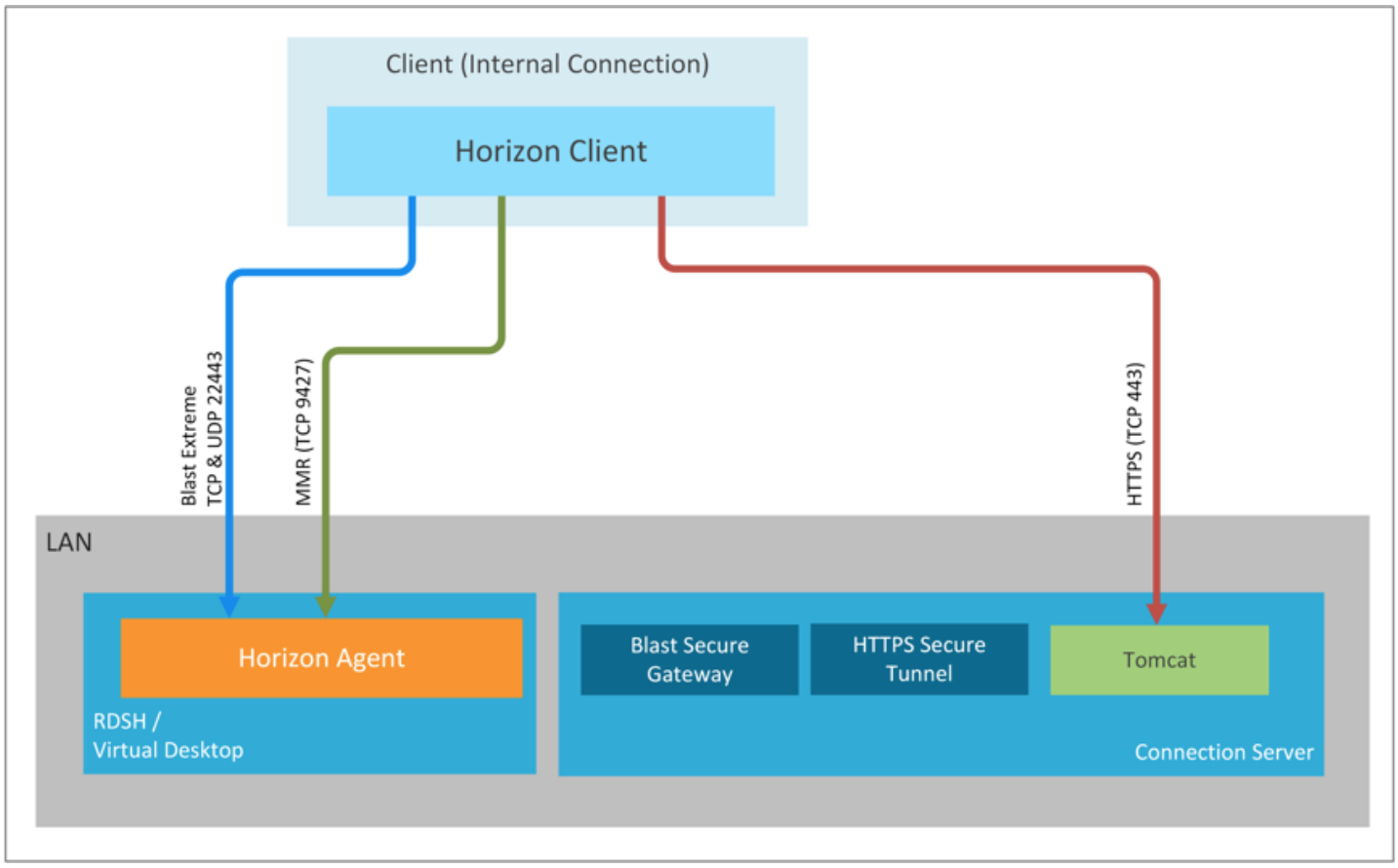

Figure 1: Internal Connection from Client to Agent Using Blast Extreme

1. Horizon Client, on the client device, connects to a Connection Server on TCP port 443 for authentication and to request a desktop or application.
2. The Connection Server returns connection information for the virtual desktop or RDS host that provides remote applications (on TCP port 443).
3. A TCP web socket connection is made on port 22443 between the client and the virtual desktop or RDS host.
   Note: At this point, the VMware Blast service on the agent side (Horizon Agent on the virtual desktop or RDS host) proxies the incoming TCP connection. The Blast Worker process determines whether UDP is enabled on the agent and allowed on the client.
4. If UDP is enabled on the agent (default), the Blast Proxy process (in Horizon Agent) attempts to make a UDP web socket connection to the client on port 22443.
   - If UDP is not enabled or is blocked, the initial TCP connection (Step 3) is used instead.
   - If LAN network conditions are detected, the initial TCP connection (Step 3) is used instead of UDP.
5. When client-drive redirection (CDR), USB redirection, or both are enabled by the administrator, by default, the traffic is side-channeled on the Blast Extreme channel.
   If desired, the traffic for each of the remote experience features between Horizon Client and Horizon Agent can be configured to use separate ports:
   - Client drive-redirection traffic can use TCP 9427.
   - USB redirection traffic can use TCP 32111.
6. If multimedia redirection (MMR) is enabled, this traffic uses TCP port 9427 between the client and agent.

Internal Tunneled Connection

With an internal tunneled connection, the client, the server, and the virtual desktop or RDS host are all also inside the corporate network, but the clients might be on a different subnet from that of the virtual desktops or RDS hosts (where the agent is installed), and you do not want to open ports between the clients and agents directly. Tunneling traffic through the Connection Server allows for ports to be open between the Connection Server and the client, and between the Connection Server and the agent, but not between the client and the agent.

The following diagram shows the ports used for an internal tunneled connection, and the list that follows describes the order in which

the connections are made.

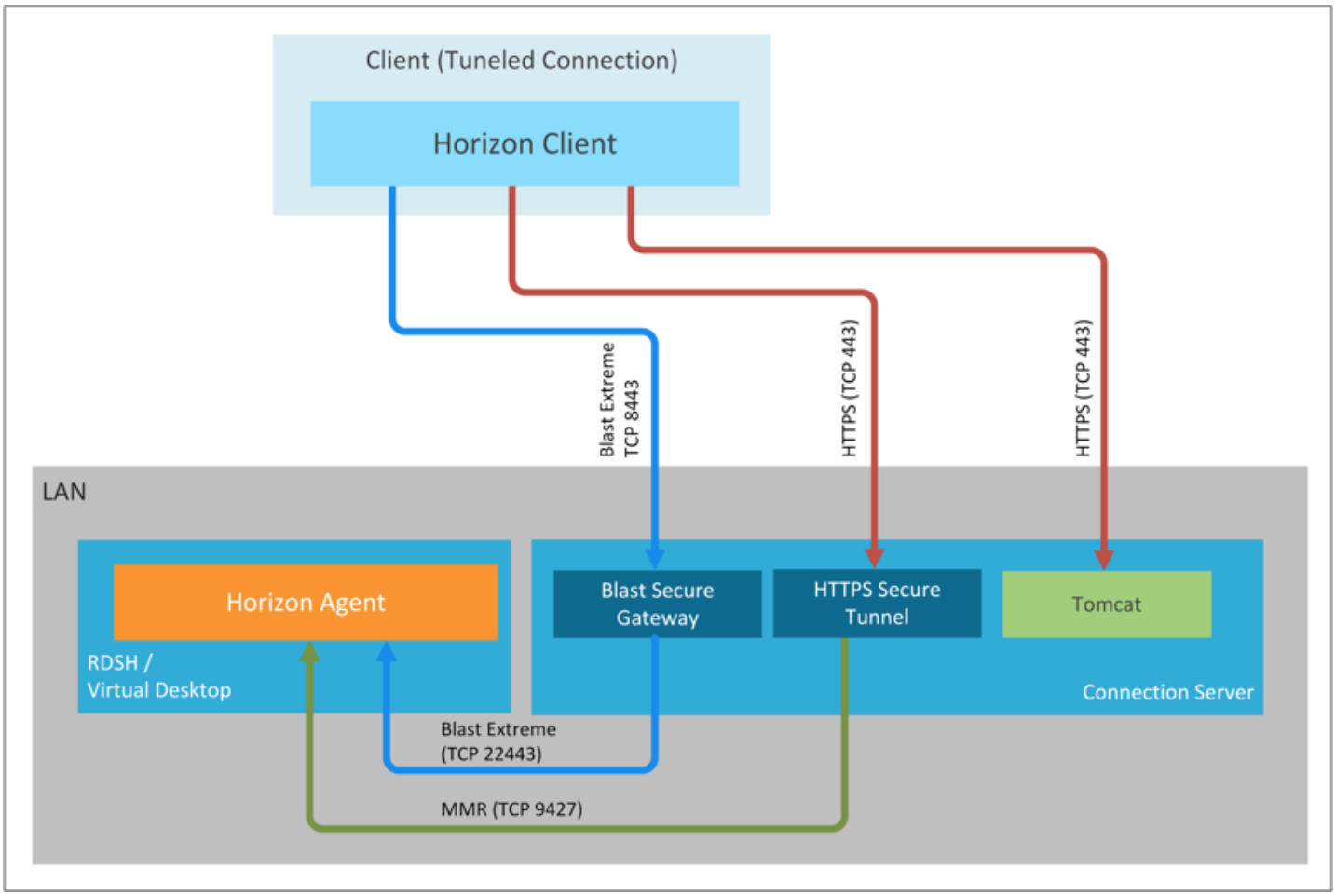

Figure 2: Tunneled Connection from Client to Agent Through the Connection Server

1. Horizon Client, on the client device, connects to a Connection Server on TCP port 443 for authentication and to request a desktop or application.
2. The Connection Server returns the connection information for the virtual desktop or RDS host that provides remote applications (on TCP port 443).
3. A TCP web socket connection is made from the client to the Blast Secure Gateway on port 443, and then from the Blast Secure Gateway to the virtual desktop or RDS host on port 22443.
4. When multimedia redirection (MMR), client-drive redirection (CDR), USB redirection, or some combination of these are enabled by the administrator, this traffic goes through the HTTPS Secure Tunnel on the Connection Server.
   TCP 443 is used between the client and the Connection Server. The traffic uses the native port for each of the remote experience features between the Connection Server and the agent:
   - Multimedia redirection traffic uses TCP 9427.
   - Client-drive redirection traffic uses TCP 9427.
   - USB redirection traffic uses TCP 32111.

External Connection

With an external connection, the client is connecting from outside the corporate network to the Unified Access Gateway. This gateway then directs the traffic to the correct port and location on the Connection Server and agent. The following diagram shows the ports used for an external connection, and the list that follows describes the order in which the connections are made.

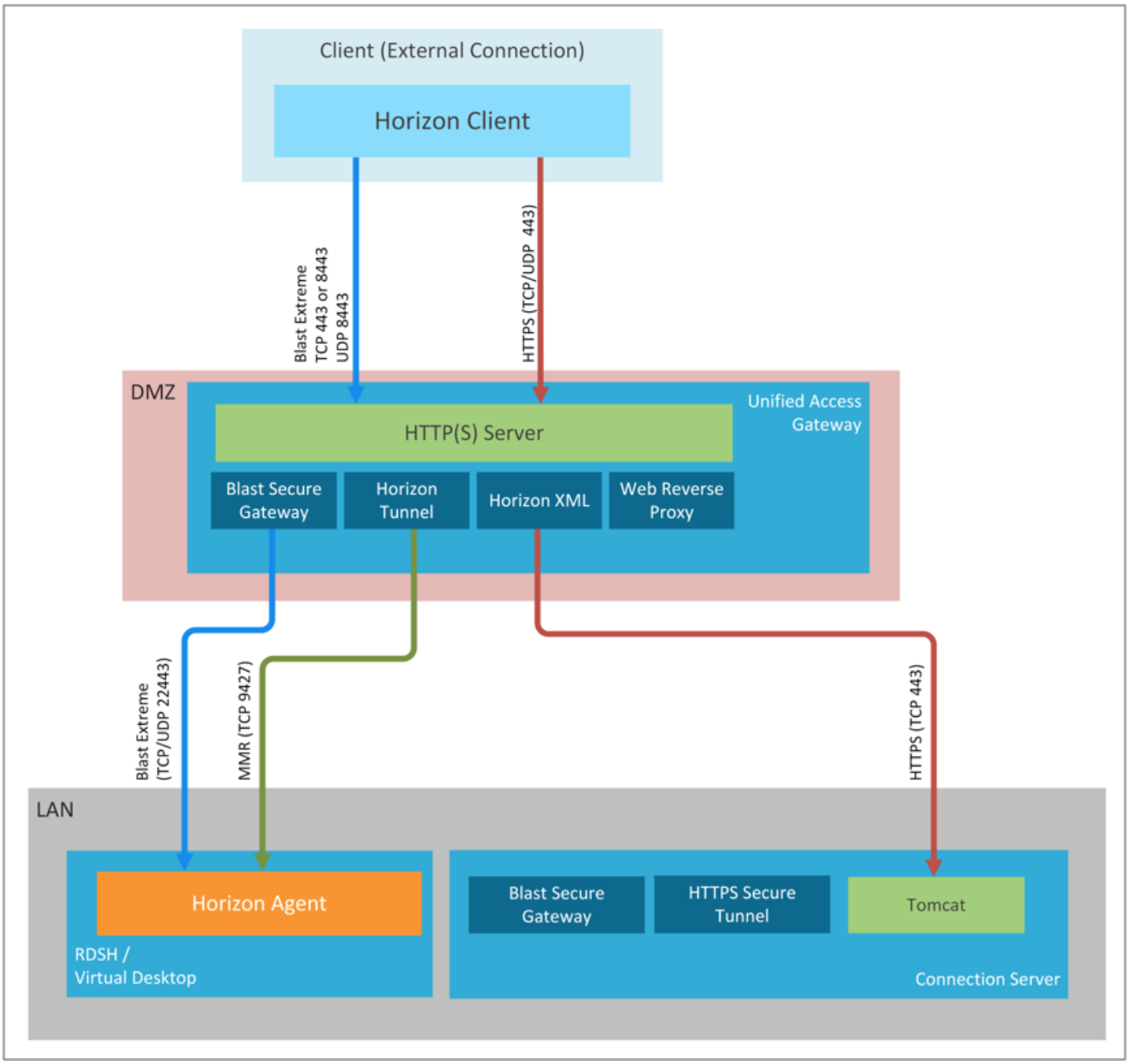

Figure 3: External Connection from Client to Agent Through the Unified Access Gateway

1. Horizon Client, on the client device, authenticates and requests a desktop or application. The connection travels from the client to a Unified Access Gateway virtual appliance on TCP port 443, and then from the Unified Access Gateway to the Connection Server on TCP port 443.
2. The Connection Server returns the connection information for the virtual desktop or RDS host to the client.
3. A web socket connection is made from the client to the Blast Secure Gateway (on the Unified Access Gateway) on TCP port 8443, and then from the Blast Secure Gateway to the virtual desktop or RDS host on TCP port 22443.
   The port used by the Blast Secure Gateway on the Unifed Access Gateway can be customized (for example, it can use TCP 443).
   Note: At this point, the VMware Blast service on the agent side (Horizon Agent on the virtual desktop or RDS host) proxies the incoming connection. The Blast Worker process determines whether UDP is enabled on the agent and allowed on the client.
4. If UDP is enabled on the agent (default), the Blast Proxy process (in Horizon Agent) attempts to make a UDP web socket connection. If UDP is not enabled or is blocked, the initial TCP connection (Step 3) is used instead.
   If LAN network conditions are detected, the initial TCP connection (Step 3) is used instead of UDP.

    1. This connection is on UDP port 8443 from the client to the UDP Tunnel on the Unified Access Gateway.
    2. The connection continues on UDP port 22443 from the Unified Access Gateway to the agent.
5. The VMware Virtual Channel is opened between the agent (virtual desktop or RDS host) and the Blast Secure Gateway on port 22443, and between the Blast Secure Gateway and the client on port 8443 using TCP or UDP as determined in Step 4. The remote experience traffic runs on this channel, including traffic related to USB redirection and client drive-redirection (CDR), if these features are enabled by the administrator.
6. When client-drive redirection (CDR), USB redirection, or both are enabled by the administrator, this traffic goes through the Horizon Tunnel on the Unified Access Gateway appliance.
   TCP 443 is used between the client and the Unified Access Gateway. By default, the traffic is then side-channeled on the Blast Extreme channel.
   If desired, you can configure the traffic for each of the remote experience features to use dedicated ports between the Unified Access Gateway and the agent:
    - Client drive-redirection can use TCP 9427.
    - USB redirection can use TCP 32111.
7. If multimedia redirection (MMR) is enabled, this traffic is not side-channeled. It uses TCP port 443 from the client to the Horizon Tunnel on the Unified Access Gateway. TCP port 9427 is then used from the Unified Access Gateway to the agent.

Security Features

Blast Extreme includes the following security features to support Horizon 7:

- **Port sharing** – If you use a Unified Access Gateway virtual appliance for connections from outside the corporate network, by default the connection uses TCP port 8443 and optionally UDP port 8443. It is possible to configure the Blast External URL on the Unified Access Gateway appliance to use port sharing on TCP port 443 so that no additional ports need be opened on the front-end firewall. There is a slight performance overhead on Unified Access Gateway if you use port sharing.
- **AES (Advanced Encryption Standard) encryption** – All TCP connections use SSL web sockets to encrypt communication. TLS 1.1 and 1.2 are supported. All UDP connections are encrypted with DTLS encryption. These encryption mechanisms apply to both the H.264 codec and the JPG/PNG codec.
- **Security certificates –** For external connections, Blast Extreme can use the security certificate on the Unified Access Gateway appliance. Blast Extreme can also use the certificate thumbprint of the Blast Secure Gateway or virtual desktop. A certificate thumbprint is a cryptographic hash of a certificate.
- **SHA-256 signatures** – Blast Extreme uses the latest security algorithms, including SHA-256.
- **IPv6 support** – You must use only TCP connections.
- **Dual IPv4/IPv6 support** – When using Blast Extreme, Unified Access Gateway can be used to bridge between IPv6 Horizon Clients and an IPv4 backend and agents. The Horizon Clients can use either IP version 4 or 6. Blast Extreme must be on TCP 443 only (as described previously for port sharing).
- **FIPS support** – FIPS-ready libraries are available for Unified Access Gateway 2.9 or later appliances.
- **Common Criteria** – The evaluation process has been initiated.

Port Requirements When Using Unified Access Gateway

The following tables summarize the port requirements.

SOURCE	PROTOCOL	PORT	DESTINATION	NOTES
Any	TCP	443	Unified Access Gateway	HTTPS for login traffic and for Blast Extreme port sharing when used.
Any	TCP	8443	Unified Access Gateway	Blast Extreme.
Any	UDP	8443	Unified Access Gateway	Blast Extreme Adaptive Transport.

Table 2: Ports Required for Outer, Front-End Firewall

SOURCE	PROTOCOL	PORT	DESTINATION	NOTES
Unified Access Gateway	TCP	443	Connection Server	HTTPS connection.
Unified Access Gateway	TCP/UDP	22443	Any desktop VM	Blast Extreme Virtual Channel.
Unified Access Gateway	TCP	32111	Any desktop VM	Optional for USB redirection. By default, USB traffic is side-channeled in the Blast Extreme port 22443. You can configure USB traffic to use the dedicated port 32111.
Unified Access Gateway	TCP	9427	Any desktop VM	Optional for client-drive redirection (CDR). Required for multimedia redirection (MMR). By default, CDR traffic is side-channeled in the Blast Extreme port 22443. You can configure CDR traffic to use port 9247. MMR must use port 9247.

Table 3: Ports Required for Inner, Back-End Firewall

Log File Locations

Log files related to Blast Extreme can be found in the following locations:

- Windows client: C:\Users\<%username%>\AppData\Local\Temp\vmware-<username>\vmware-mks-<#>.log
- Mac client: Users/<%username%>/Library/Logs/VMware/vmware-mks-<#>.log

To collect logs on a Mac, you can use the Horizon Collector for Mac Fling (which like all VMware flings, is not officially supported).

- Horizon Agent:
  <Drive>:\ProgramData\VMware\VMware Blast\
  This directory contains logs for the three Blast Extreme components:
  - Blast-Service.log
  - Blast-Worker-SessionId<#>.txt
  - Blast-Proxy.log

For more information about the entries in these log files, see Verifying Successful Configuration.

Deployment

To set up the Horizon 7 environment for Blast Extreme, administrators open the front-end firewall ports and select Blast Extreme as the default display protocol or as a possible protocol choice for end users.

Software and Port Requirements

Use the correct version of Horizon 7 and related components:

- Connection Server 7.1 or later.
- For external connections: Unified Access Gateway 2.9 or later.
- Horizon Clients 4.8 or later are recommended because these versions include the Blast Extreme Network Intelligent Transport (BENIT) networking stack, which dynamically chooses between TCP and UDP, depending on network conditions. See the BENIT FAQ section. (Horizon Client 4.0 and later support Blast Extreme, but newer versions introduce more features and

performance improvements.)
- Horizon Agent 7.5 or later is recommended because these versions include the Blast Extreme Network Intelligent Transport (BENIT) networking stack. (Horizon Agent 7.0 and later support Blast Extreme, but newer versions introduce more features and performance improvements.)
- For Linux desktops: Horizon for Linux version 7 (or later); 7.3 or later to use the H.264 codec; 7.5 or later to use the Network Intelligence transport.

Configuration Settings for Administrators

To use Blast Extreme, you must verify that the Blast Extreme display protocol is selected in the Horizon Administrator UI.

- In the pool settings (desktop pool or application pool), for **Remote Display Protocol**, you can select **VMware Blast** as the default display protocol, or you can specify that users can choose the protocol. See Setting Up Virtual Desktops in Horizon 7 or Setting Up Published Desktops and Applications in Horizon 7.
- In Horizon Administrator, you can also configure the remote display protocol at the RDSH-farm level. For more information, see Setting Up Published Desktops and Applications in Horizon 7.
- To configure the remote display protocol at the global-entitlement level, see Administering Cloud Pod Architecture in Horizon 7.

Configuring Advanced Settings Using Group Policy Settings

For most advanced settings, you can use the vdm_blast.admx group policy template. The group policy templates are included in the VMware-Horizon-Extras-Bundle-xxx.zip GPO bundle file.

The following list includes only a few of the settings included in the policy template:

- Bandwidth and frame rate settings Note: For guidance about using these settings, see Performance Tuning for Various Network Conditions.
- Whether to use UDP transport
- Whether to use the H.264 codec
- Nondefault port number to use for HTTP service (default: 22443)
- Image quality settings for the JPG/PNG and H.264 codecs
- Copy and paste (Clipboard redirection) capabilities between client and virtual desktop

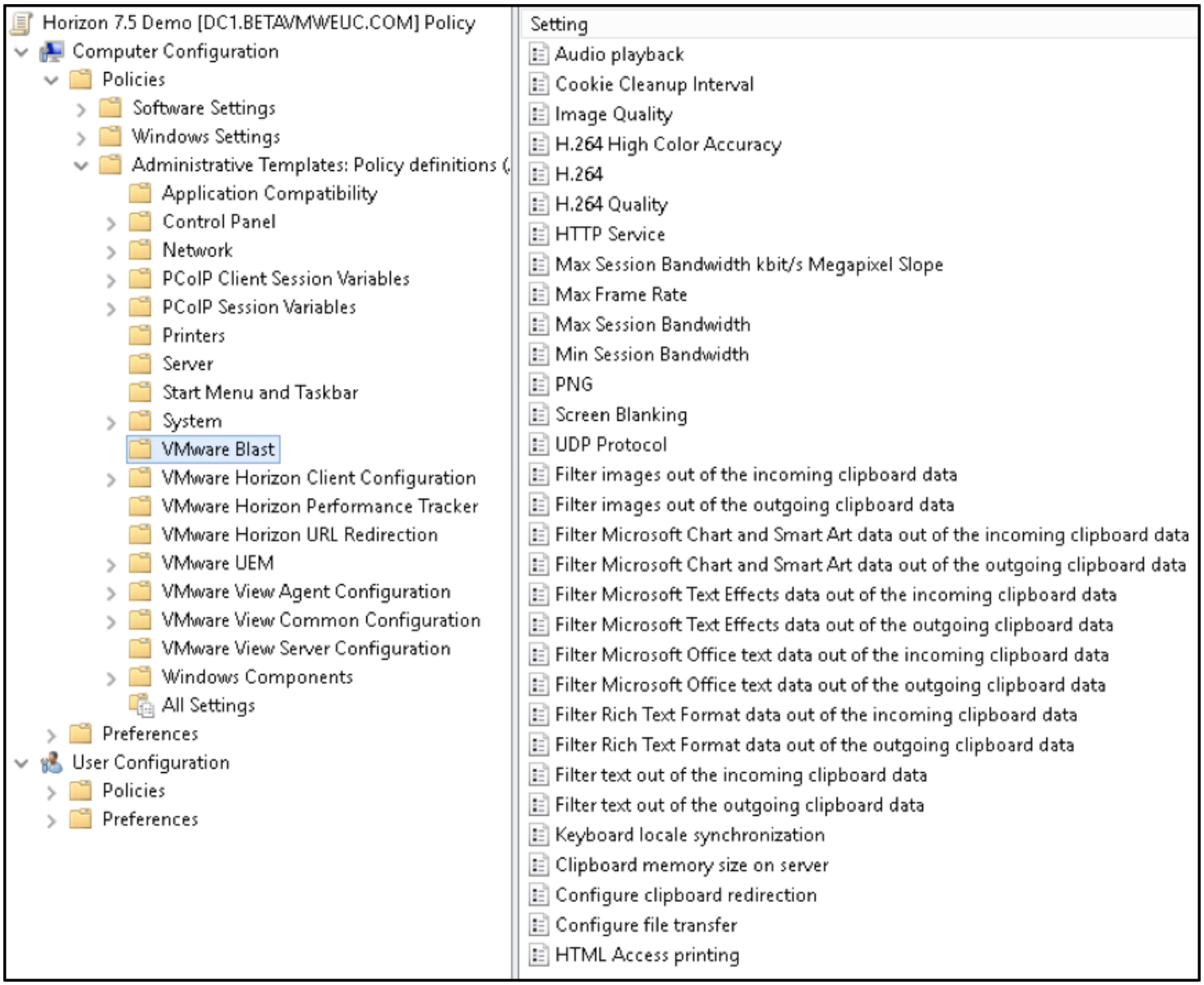

Figure 4: GPO Settings for Blast Extreme

Note: For Horizon Agent 7.0.1 and later, profiles are available that automatically configure the abovementioned settings based on particular use cases.

For more information about the specific group policy settings, see *VMware Blast Policy Settings* in Configuring Remote Desktop Features in Horizon 7. For instructions on importing the template, see *Add Horizon 7 ADMX Template File to a GPO*, in Configuring Remote Desktop Features in Horizon 7.

Bandwidth Profiles Available with Horizon 7 Smart Policies
With User Environment Manager 9.1 or later and Horizon Agent 7.0.1 or later, you can create Horizon 7 Smart Policies that apply different bandwidth profiles to different users based on user location and network speed. You can choose from bandwidth profiles such as high-speed LAN, LAN, and low-speed WAN to prevent the virtual desktop or RDS host from attempting to transmit data at a higher rate than the link capacity.

For details about the profiles, see the profile reference topic in the *Using Smart Policies* section of Configuring Remote Desktop Features in Horizon 7.

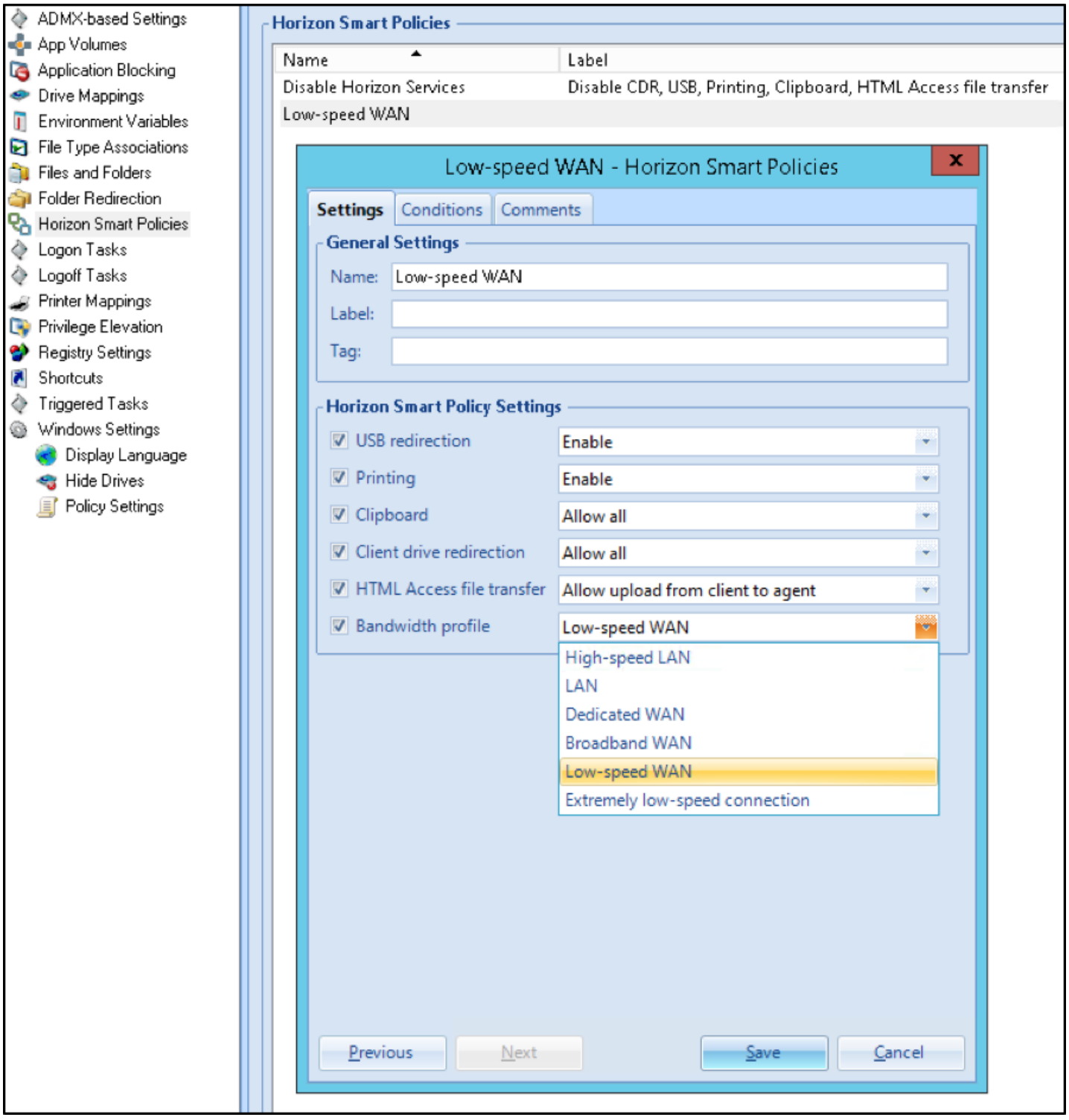

Figure 5: User Environment Manager Horizon Smart Policies

Configuring Images to Build to Lossless

To configure lossless compression for use cases such as medical imaging, you must set the appropriate value in a Windows Registry key on the virtual desktop or RDS host where Horizon Agent is installed.

1. Open the Windows Registry Editor (regedit.exe) on the agent machine and navigate to the following folder: HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config
2. In the Config folder, if the key named **EncoderBuildToPNG** does not already exist, create it, and set it to **1**.

The default value is 0 (disabled), which means the codec does not build to PNG, a lossless format. Note: Enabling lossless compression causes an increase in bandwidth and CPU usage. Configuration changes to this dynamic key take effect immediately.

Configuration Settings for End Users

If you give end users a choice of display protocols, they can select Blast Extreme as their preferred protocol. If you configure Blast Extreme and do not give end users a choice, then if clients try to connect using a version of the client that is earlier than Horizon Client 4.0, the Connection Server falls back to having the client connect with PCoIP. Blast Extreme is not supported for pre-4.0 clients. Similarly, end users with PCoIP-supported zero clients are automatically connected with PCoIP. For a list of zero and thin clients that support Blast Extreme, see the VMware Compatibility Guide.

End users using Blast Extreme can also configure whether to allow use of the H.264 codec. The clientside settings can be applied only if the administrator allows the environment to use H.264. If the administrator configures the environment to use the JPG/PNG codec, then even if the end user turns on **Allow H.264 decoding**, that codec is not used.

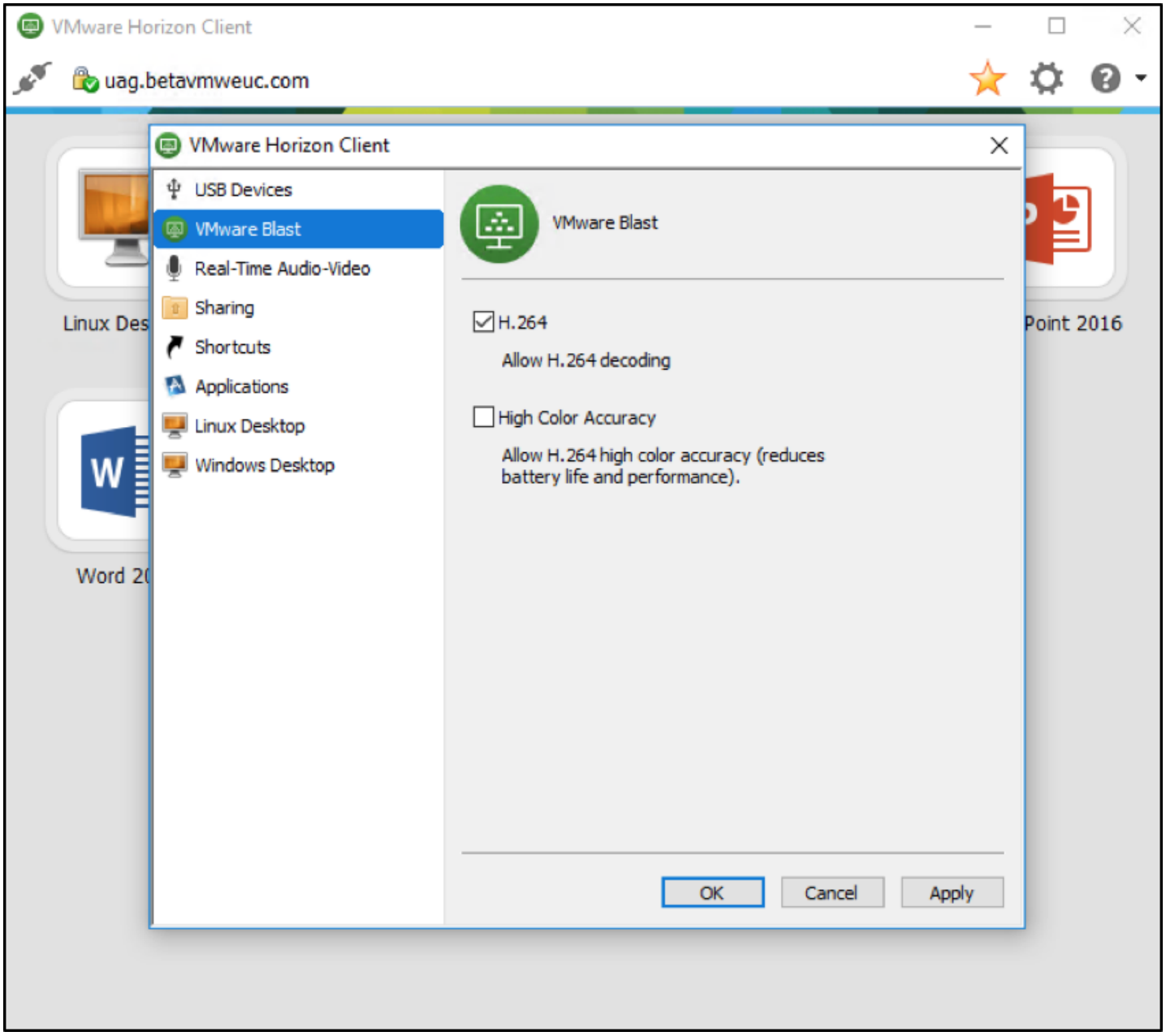

Figure 6: Horizon Client Configuration Options

With Horizon Client 4.0–4.3 are different from those for Horizon Client 4.7 and later, users have the option to enable **High Color**

Accuracy, which allows increased color fidelity when using H.264 decoding. Administrators can configure this setting by using the H.264 High Color Accuracy group policy setting, as shown in the following figure.

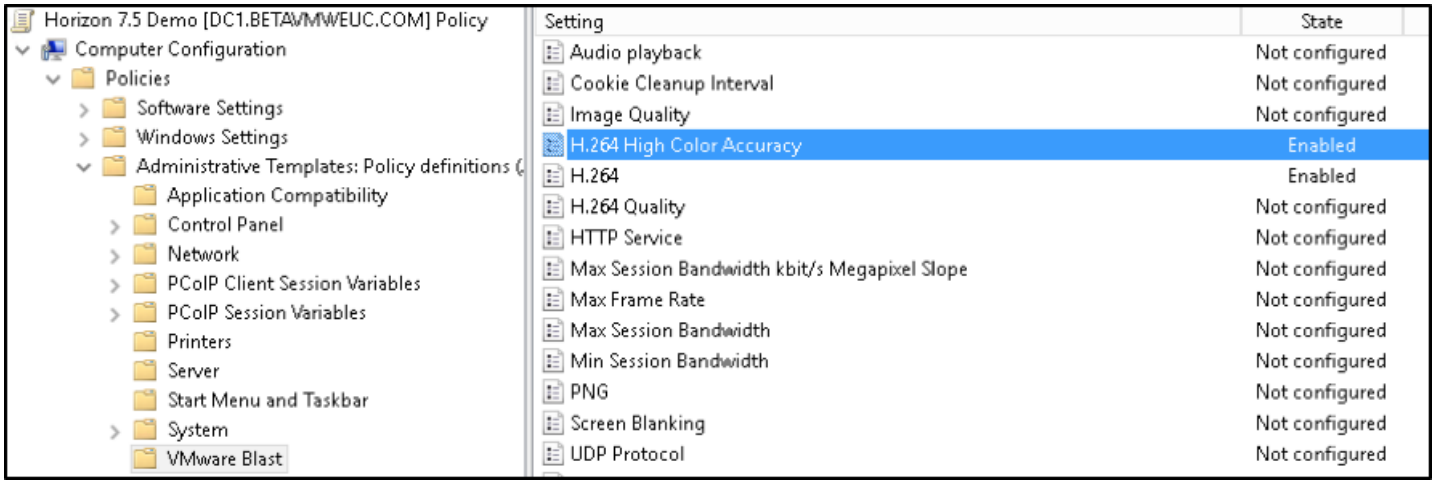

Figure 7: Group Policy Setting for H.264 High Color Accuracy

By default, H.264 uses 4:2:0 chroma subsampling, but this setting is not optimal for certain color combinations. For example, some applications default to red text on blue, leading to "blocky" text that is difficult to read. Other use cases include high-end graphics apps such as 3D CAD/CAM and medical images where higher color depth is required. Enabling the High Color Accuracy setting causes H.264 to use chroma 4:4:4 subsampling. A comparison is shown in the following figure.

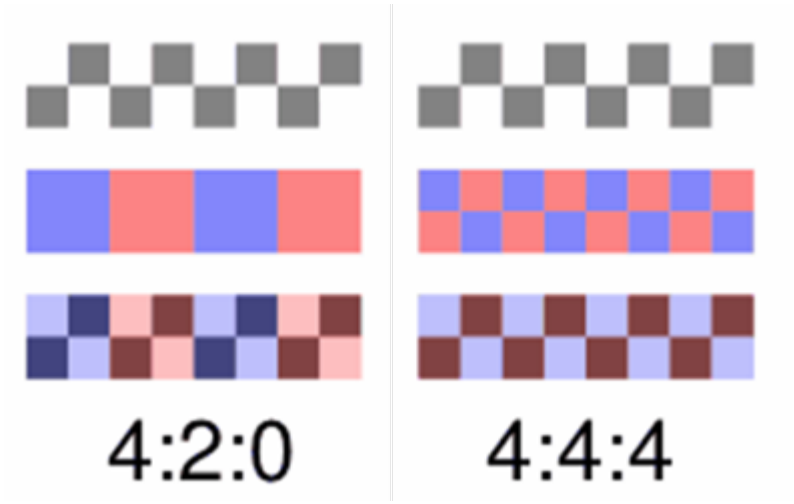

Figure 8: Chroma Subsampling Comparison

Note, however, that high color accuracy can reduce battery life and incur some performance overhead on the client and network connection.

Blast Extreme Network Intelligent Transport (BENIT)

In clients prior to Horizon Client 4.8, users were required to choose from three options to describe their network conditions, namely **Excellent**, **Typical**, and **Poor**.

With Horizon Client 4.8, these three options have been removed from all native clients except Horizon Client for Windows 10 UWP. The Blast Extreme networking stack now dynamically chooses the right mode. This built-in intelligence is called Blast Extreme Network Intelligent Transport (BENIT).

1. **Question**: If you used to choose **Excellent** mode in the client UI to force TCP, now that this option is no longer available, how do you force TCP?

Answer: Use the registry key `HKLM\SOFTWARE\Policies\VMware, Inc.\VMware Blast\Config`, and set `UdpEnabled` to to force TCP. For the changes to take effect, restart the agent. This registry key is present in all versions of Horizon Agent, starting from Horizon 7 version 7.0.

2. **Question**: If you used to choose **Typical** mode in the client UI to force UDP Adaptive Transport, now that this option is no longer available, how do you force UDP Adaptive Transport?
   Answer: **Typical** mode did not always guarantee that UDP would be used. **Typical** mode would use UDP Adaptive Transport if it was available. If you want to ensure that the connection does not try to switch back to TCP, you can use the registry key `HKLM\SOFTWARE\Policies\VMware, Inc.\VMware Blast\Config`, and set `NetworkIntelligenceEnabled` to to get legacy **Typical** mode/Adaptive Transport connection. For the changes to take effect, you need to log off from the agent and log in again.
3. **Question**: If TCP and UDP Adaptive Transport are dynamically chosen at the backend, how do you know which protocol is actually used?
   Answer: Use VMware Horizon Performance Tracker (PerfTracker), a monitoring tool, to determine which transport is being used.
   Performance Tracker can be selected as an option and installed as part of the Horizon Agent installation. A shortcut to the Performance Tracker executable appears on the desktop.
4. **Question**: If all the three options are removed in the client UI, how does a new client work with already released agents and brokers?
   Answer: BENIT needs both the client and the agent to be at a certain minimum version. The client must be Horizon Client 4.8 or later, and the agent must be Horizon Agent 7.5 or later. If the client meets the minimum version requirement but the agent does not, the client will, by default, try to connect using **Typical** mode, provided agent has UDP enabled as noted in question 2. If you want to use **Excellent** mode, refer to question 1.
5. **Question**: Which clients are affected? Are there still clients that have the old three options?
   Answer: All native clients adopted BENIT in the 4.8 release except Horizon Client for Windows 10 UWP.
6. **Question**: Which agent operating systems are affected by this change?
   Answer: Windows and Linux operating systems in the Horizon 7 version 7.5 release.
7. **Question**: As a debugging step, how do you disable BENIT?
   Answer: On the agent side, use the registry key `HKLM\SOFTWARE\Policies\VMware, Inc.\VMware Blast\Config`, and set `NetworkIntelligenceEnabled` to . For the changes to take effect, log off from the agent and log in again.
   On desktop clients you can disable BENIT by adding `RemoteDisplay.enableBlastNetworkIntelligence=FALSE` to a configuration file:

- For Horizon Client for Windows, use the following file: `C:\ProgramData\VMware\VMware Horizon View\config.ini`

- For Horizon Client for macOS, use the following file: `~/Library/Preferences/VMware Horizon View/config`
- For Horizon Client for Linux, use the following file: `/etc/.VMware/config`

Client Device Support for the H.264 Codec

Horizon Client 4.0 and later support H.264 software encoding and hardware decoding on the following types of client devices:

- Most laptops and PCs manufactured in 2013 or later
- Chromebooks
- iOS and Android devices
- Windows tablets and phones

For Macs, Horizon Client 4.2 and later support hardware decoding. Horizon Client for macOS 4.0 and 4.1 support H.264 software decoding. For HTML Access, this feature is supported on Chrome browsers
(version 45 or later) if the device supports H.264 decoding. For other browsers, the JPG/PNG codec is used.

For feature support in versions of Horizon Client version 4.0 and later, see the release notes on the VMware Horizon Clients Documentation page.

Verifying Successful Configuration

To verify that the Blast Extreme display protocol is being used for a specific session:

- In Horizon Administrator, on the Sessions tabs that provide a list of desktop, application, or RDSH sessions, look for the Display Protocol column, which shows which protocol is used for each session.
- In the Windows Registry of the virtual desktop or RDS host, in the list of volatile variables, look for the ViewClient_Protocolvariable, which shows which protocol is being used. The path to this variable is HKEY_LOCAL_MACHINE\Software\VMware, Inc. \VMware VDM\SessionData\<n>, where <n> is the number of the session.

To verify which transport protocol is selected, look in the Blast-Service.log file, located in the virtual desktop or RDS host in the <Drive>:\ProgramData\VMware\VMware Blast\ directory. This log contains entries that indicate whether UDP or TCP is being used. Search for entries with the text Protocol for Session.

To verify which codec is selected, look in the Blast-Worker-SessionId<#>.txt file, located in the virtual desktop or RDS host in the <Drive>:\ProgramData\VMware\VMware Blast\ directory. Search for entries with the text VNCEncodeChooseRegionEncoder. If this text is followed by region encoder H.264, the H.264 codec is being used. If the text says region encoder adaptive, the JPG/PNG codec is being used.

To verify which codec is actually being used on the client device, look in the log file for the specific log entry:

- On Windows clients, look in the log file for entries that contain the text H.264. The file location is C:\Users\<%username%>\AppData\Local\Temp\vmware-<username>\vmware-mks-<#>.log.
- On Mac clients, look in the log file for entries that contain the text H264. The file location is Users/<%username%>/Library/Logs/VMware/vmware-mks-<#>.log.

Optimization Tips

Several tools are available to help you optimize your environment for Blast Extreme.

General Recommendations

To get the best performance with Blast Extreme in low-bandwidth, high-latency situations, VMware recommends the following configuration settings:

- Verify that you are using Horizon 7 version 7.5 or later and Horizon Client 4.8 or later.
- Classify Blast Extreme network traffic as interactive real-time traffic, just below VoIP, but above all other TCP-based traffic. That is, prioritize Blast Extreme in the same way that you prioritized PCoIP if you previously used PCoIP.
- If your end users do not require client-drive redirection (CDR), do not enable this feature.
- Windows-specific optimizations include the following:

  - Use the VMware OS Optimization Tool Fling default template to disable a number of items.
  - Use the OS Optimization Tool to also disable the following Windows features: Dynamic Windows Preview, Taskbar Animation, and Windows Peek.
  - Use Group Policy to prohibit Desktop Wallpaper.

Performance Tuning for Various Network Conditions

The default settings should suffice for most use cases and network conditions. In extremely poor network conditions, usability and user experience might be enhanced by tuning parameters that are specific to the issue causing the network problem:

- Low bandwidth
- High latency
- High rate of dropped packets

Low Bandwidth

The following GPO settings are especially helpful in low-bandwidth conditions:

- **Max Bandwidth Slope for the Kbps Per Megapixel** – Defines a limit for the bandwidth that the Blast Extreme display traffic can consume. Lower this value to reduce the amount of pixel information sent.
  Values as low as 1000 have provided bandwidth benefits while still providing a good user experience, but be sure to test any changes you make to determine the impact on user experience.
  Note: This setting is not a hard limit, as stability and usability of the session are prioritized over a strict bandwidth cap when necessary.
- **Max Session Bandwidth** – Defines a limit for the total bandwidth consumed by the session, including Blast Extreme traffic and traffic used by remote-experience features such as client-drive redirection, USB redirection, printing, and audio.
  This setting does not take into account the virtual desktop resolution and the number of pixels being remoted. Therefore, applying a fixed bandwidth limit on a single display versus a dual display, or a 1280x768 resolution versus a 1920x1080 resolution, for example, can greatly impact the performance of the display protocol and user experience.
  Too low a value can hamper performance if a remote-experience feature such as USB redirection consumes too much of the allotted session bandwidth. Try tuning this setting if tuning the **Max Bandwidth Slope for the Kbps Per Megapixel** setting does not provide all the performance improvements you require.
  Note: This setting is not a hard limit, as stability and usability of the session are prioritized over a strict bandwidth cap when necessary.
- **Max Frame Rate** – Defines the maximum number of display frames per second that are delivered by the session. This setting helps to manage the average bandwidth consumed by limiting the number of screen updates per second.

For more information about these group policy settings, see *VMware Blast Policy Settings* in the Horizon 7 documentation.

In situations where bandwidth is constrained, you can also take the following actions to reduce the amount of traffic transmitted:

- Decrease the display resolution.
- Ensure that the OS image has been optimized. Use the VMware OS Optimization Tool Fling.
- If the use case does not require audio, block audio playback using the **Audio playback** GPO setting. Transmitting system sounds causes unnecessary bandwidth consumption.
- If the use case does not require certain functionality such as client-drive redirection, USB redirection, or printing, disable it.
- If Adobe Flash content is used, consider configuring the Flash redirection feature. This feature transmits the Flash stream and processes it on the client, thereby reducing the bandwidth consumed. See *Configuring Flash Redirection*, in the Horizon 7 documentation.
- Use URL Content Redirection to configure certain sites to open on the client side. This feature can be beneficial where a site is non-work-related and opening it in the virtual desktop would consume unnecessary resources on the VM and consume bandwidth by transmitting URL content to the client. See *Configuring URL Content Redirection*, in the Horizon 7 documentation.
- Use the GPO clipboard settings to reduce or block copying images, graphics, and rich text.

High Latency

Blast Extreme has been observed to work well in environments with latency greater than 300 milliseconds. Although you cannot lower the latency of the physical network connection, you can reduce the amount of traffic being sent.

Blast Extreme and other remote display protocols with low-latency connections (that is, less than 50 ms round trip) can easily maintain acceptable levels of user experience without the need for tuning. User IO operations (keyboard, mouse) are impacted by latency.

Connections with 300 ms of round-trip latency equate to a one-third of a second delay every time a key is pressed or a mouse button is clicked. The lower the network latency, the better the user experience.

High latency has another impact on remote display performance. Network bandwidth is limited when high latency is present—this is referred to as “effective bandwidth.” Effective bandwidth is the actual speed at which data can be transmitted over a connection. This is in contrast to the theoretical maximum that the connection can provide. Some users with bandwidth connections that are advertised as 10 Mbps might have only 1.5 Mbps accessible due to high amounts of latency. In that case, the user workload might require 3 Mbps during peak usage.

Remote display protocol performance will degrade when bandwidth is strapped. The frame rate will drop and the display will become less responsive. Files will take longer to transmit through client-drive redirection, print jobs will take longer to print, and so on. Blast Extreme has been designed to work efficiently under constrained network conditions and can be tuned accordingly. However, there is no substitute for ample bandwidth, low latency, and low packet-loss connectivity.

Follow the guidance for low-bandwidth conditions and prioritize the content being remotely delivered.

Packet Loss
On network connections that suffer from a high percentage of dropped packets, Blast Extreme is generally able to cope with considerable packet loss. UDP is better at handling packet loss than TCP. UDP can deliver a good user experience in conditions of up to 20 percent packet loss.

- Use the Unified Access Gateway 2.9 or later.
- Ensure that UDP is configured end to end and that the necessary ports are open.
- Make sure that the default UDP configuration has not been changed in the agent.
- se Horizon Client 4.8 or later and Horizon Agent 7.5 or later. These versions include the Blast Extreme Network Intelligent Transport (BENIT) networking stack, which dynamically chooses between TCP and UDP, depending on network conditions. In packet loss situations, UDP will be used when possible. See the BENIT FAQ section.

Using Windows Performance Counters

The following Windows performance counters (Perfmon) are available:

- Estimated bandwidth
- Estimated FPS (frames per second)
- Estimated RTT (round-trip time/latency)
- Estimated throughput

Note: VMware vRealize® Operations for Horizon® supports the collection of Blast Extreme data if you are using Horizon Agent 7.0.1 or later. Additionally, with Horizon 7 version 7.5, the VMware Horizon Performance Tracker utility can monitor the performance of the display protocol.

Additional Resources

Horizon 7 Administration

Configuring Remote Desktop Features in Horizon 7

VMware Horizon Client documentation

VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture

Network Ports in VMware Horizon 7

VMware Unified Access Gateway Documentation

Deploying Hardware-Accelerated Graphics with View Virtual Desktops

VMware Horizon Blast Extreme Acceleration with NVIDIA GRID blog post

VMware Windows Operating System Optimization Tool Guide

About the Authors and Contributors

Graeme Gordon is a Senior Staff End-User-Computing Architect, EUC Technical Marketing, VMware.

Caroline Arakelian is a Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware.

Chris Halstead co-authored the original version of this white paper. Chris is EUC Staff Architect, End-User-Computing Technical Marketing, VMware.

The authors wish to thank the following people for their contributions to this paper:

- Frank Anderson, EUC Architect, EUC Technical Marketing, VMware
- Josh Spencer, EUC Architect, EUC Technical Marketing, VMware
- Ramu Panayappan, Director, Virtual Workspace R&D, VMware
- Mike Oliver, Staff Engineer, Virtual Workspace R&D, VMware
- Salil Kanitkar, Senior Member of the Technical Staff, Virtual Workspace R&D, VMware
- Mark Ewert, Lead Technologist, EUC Competitive Marketing, VMware
- Matt Coppinger, Director, Technical Marketing and Enablement, EUC Technical Marketing, VMware

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

HZN75

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com