DOCUMENT – JUNE 2021

PRINTED 28 JUNE 2021

NETWORK PORTS IN VMWARE HORIZON 7

vmware®

Table of Contents

Network Ports in VMware Horizon 7

About This Guide

This document lists port requirements for connectivity between the various components and servers in a VMware Horizon 7 deployment. This document applies to all versions of Horizon 7 from 7.0 onwards.

- For Horizon 8, see Network Ports in VMware Horizon.
- For Horizon Cloud Service on Microsoft Azure, see VMware Horizon Cloud Service on Microsoft Azure Network Ports Diagrams.

Horizon 7 Network Ports with All Connection Types and All Display Protocols

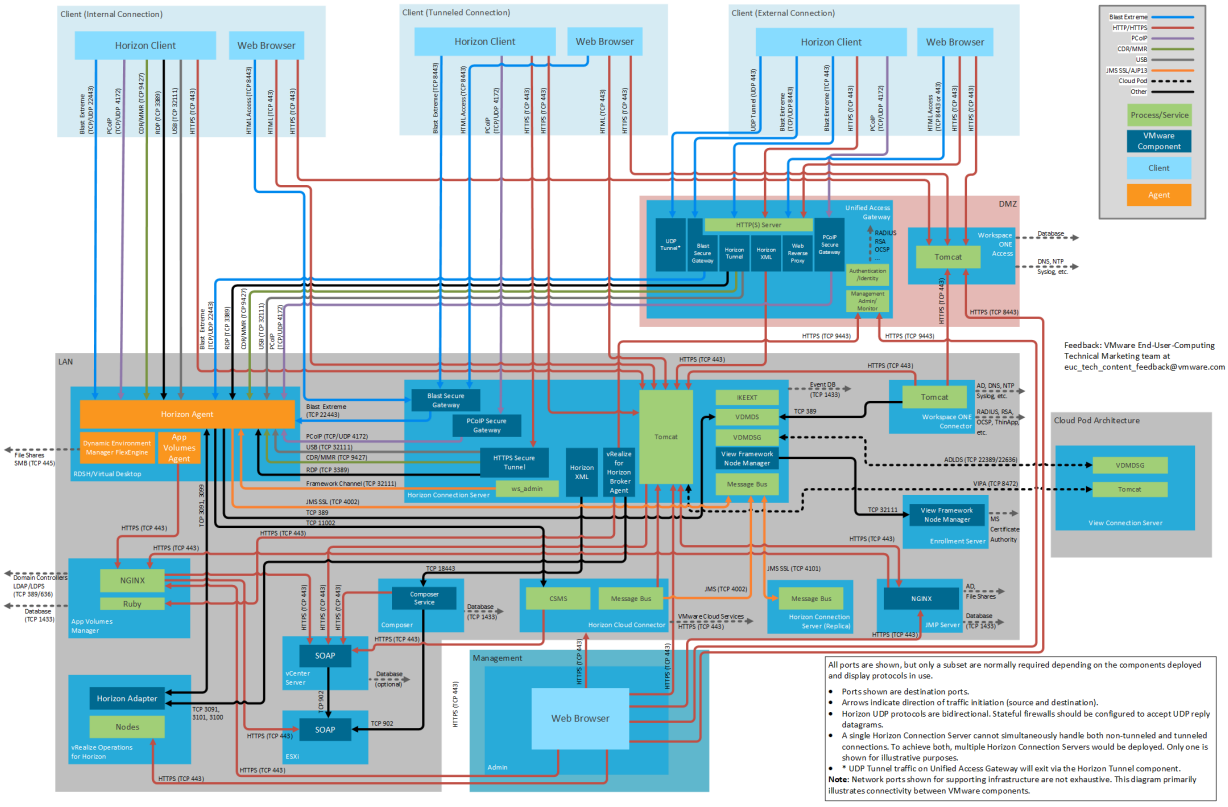


Figure 1: Horizon 7 Network Ports with All Connection Types and All Display Protocols

Figure 1 shows three different client connection types and also includes all display protocols. Different subsets of this diagram are displayed throughout this document.

Each subset of Figure 1 focuses on a particular connection type and display protocol use.

The embedded diagrams (and those in the pdf) are screen resolution versions. If higher resolution and the ability to zoom is required, for example to print as a poster, click on the desired diagram using the online HTML5 version of this document. This will open a high-resolution version which can be saved, opened in an image viewer, and printed.

This document also contains tables that list all possible ports from a source component to destination components. This does not mean that all of these ports necessarily need to be open. If a component or display protocol is not in use, then the ports associated with it can be omitted. For example:

- If Blast Extreme is the only display protocol used, the PCoIP ports need not be opened.
- If vRealize Operations for Horizon is not deployed, ports to and from it can be ignored.

Ports shown are destination ports. The source and destination indicate the direction of traffic initiation.

Horizon UDP protocols are bidirectional. Stateful firewalls should be configured to accept UDP reply datagrams.

The Horizon 7 tables and diagrams include connections to the following products, product families, and components:

- vRealize Operations for Horizon
- VMware Horizon Client™
- VMware Workspace ONE Access™ (formerly VMware Identity Manager)
- VMware Unified Access Gateway™
- VMware App Volumes™
- VMware Dynamic Environment Manager™ (formerly User Environment Manager)
- VMware vCenter Server®
- VMware ESXi™
- VMware ThinApp®

Client Connections

Network ports for connections between a client (either Horizon Client or a browser) and the various Horizon 7 components vary by whether the connections are internal, external, or tunneled.

Internal Connection

An internal connection is typically used within the internal network. Initial authentication is performed to the Horizon Connection Server, and then the Horizon Client connects directly to the Horizon Agent running in the virtual desktop or RDS Host.

The following table lists network ports for internal connections from a client device to Horizon 7 components. The diagrams following the table show network ports for internal connections, by display protocol.

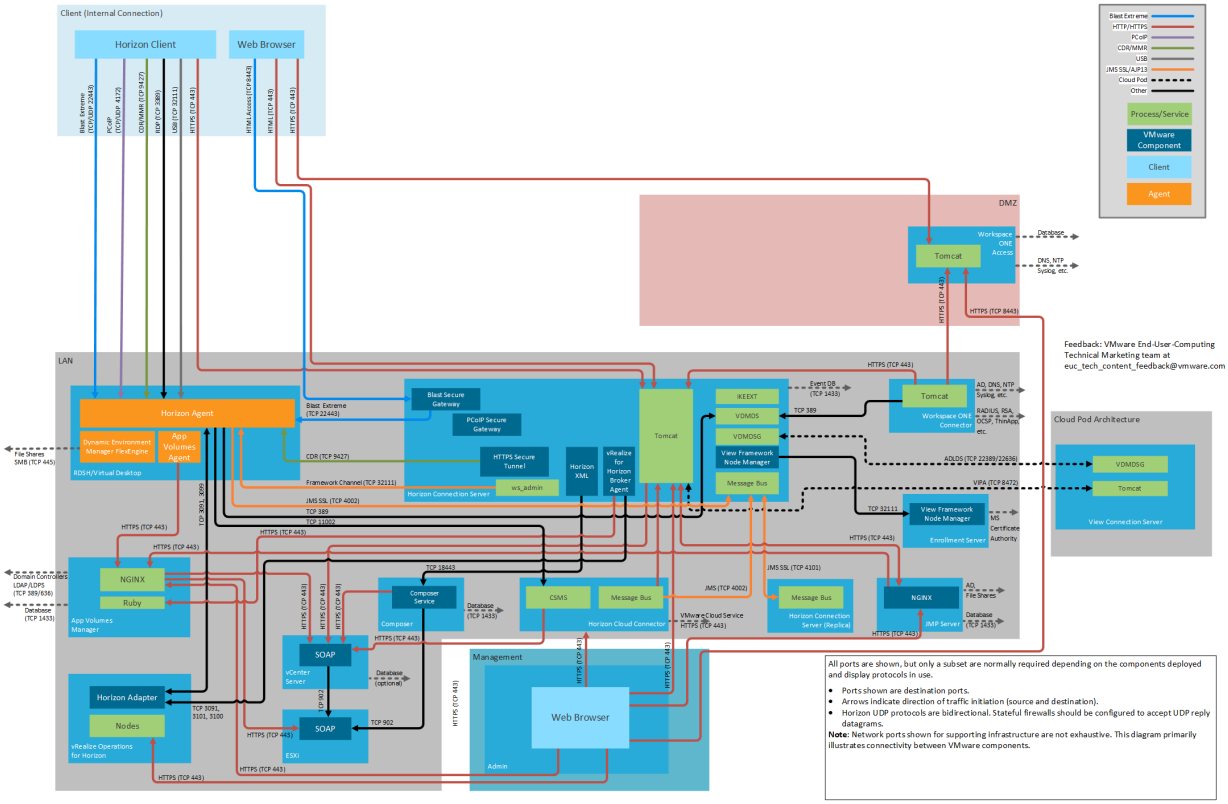
Source	Destination	Network Protocol	Destination Port	Details
Horizon Client	Horizon Connection Server	TCP	443	Login traffic. SSL (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in some cases. See *HTTP Redirection in Horizon 7* in Horizon 7 Security.
	Horizon Agent	TCP	22443	Blast Extreme.
		UDP	22443	Blast Extreme.
		TCP	4172	PCoIP.
		UDP	4172	PCoIP.
		TCP	3389	RDP.
		TCP	9427	Windows multimedia redirection, client drive redirection, HTML5 multimedia redirection, Microsoft Teams optimization, VMware printer redirection, and USB redirection. By default, when using Blast Extreme, CDR traffic is side-channeled in the Blast Extreme ports indicated previously.
		TCP	32111	Optional for USB redirection. USB redirection traffic can also be side-channeled in the Blast Extreme ports indicated previously. See note below.
Browser	Horizon Connection Server	TCP	8443	Horizon 7 HTML Access.
	Workspace ONE Access Appliance	TCP	443	Workspace ONE Access login and data traffic.
		Both	88	iOS single sign-on (SSO).
		TCP	5262	Android single sign-on (SSO).
		TCP	7443	SSL certificate authentication.
	Workspace ONE Access Connector	TCP	443	This port is required only for a connector being used in inbound mode (outbound mode is recommended). If Kerberos authentication is configured on the connector, this port is required.

Notes:

With the VMware Blast display protocol, you can configure features, such as USB redirection, and client drive redirection, to send side channel traffic over a Blast Extreme ports. See:

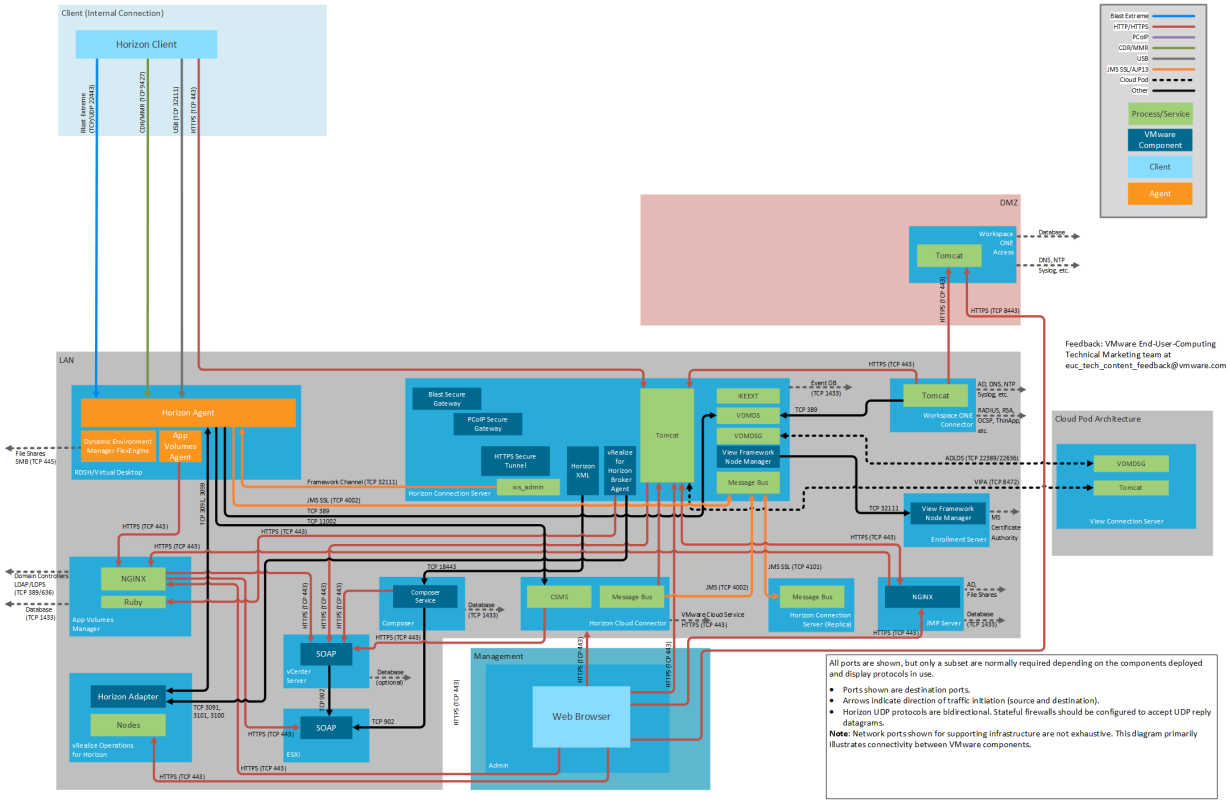
- Enabling the USB Over Session Enhancement SDK Feature.
- Managing Access to Client Drive Redirection.

Internal Connection Showing All Display Protocols



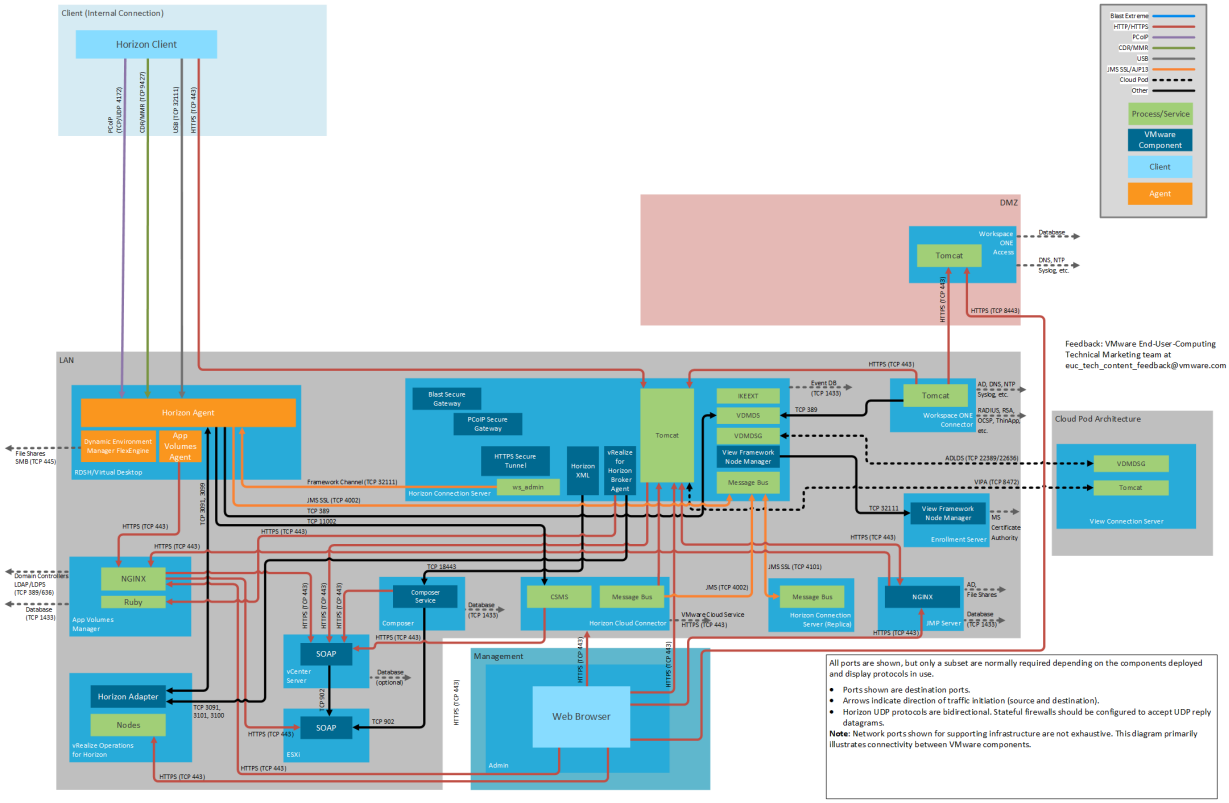
2021-06-28 Rev **Figure 2:** Internal Connection Showing All Display Protocols

Blast Extreme Internal Connection



2021-06-28 Rev **Figure 3:** Blast Extreme Internal Connection

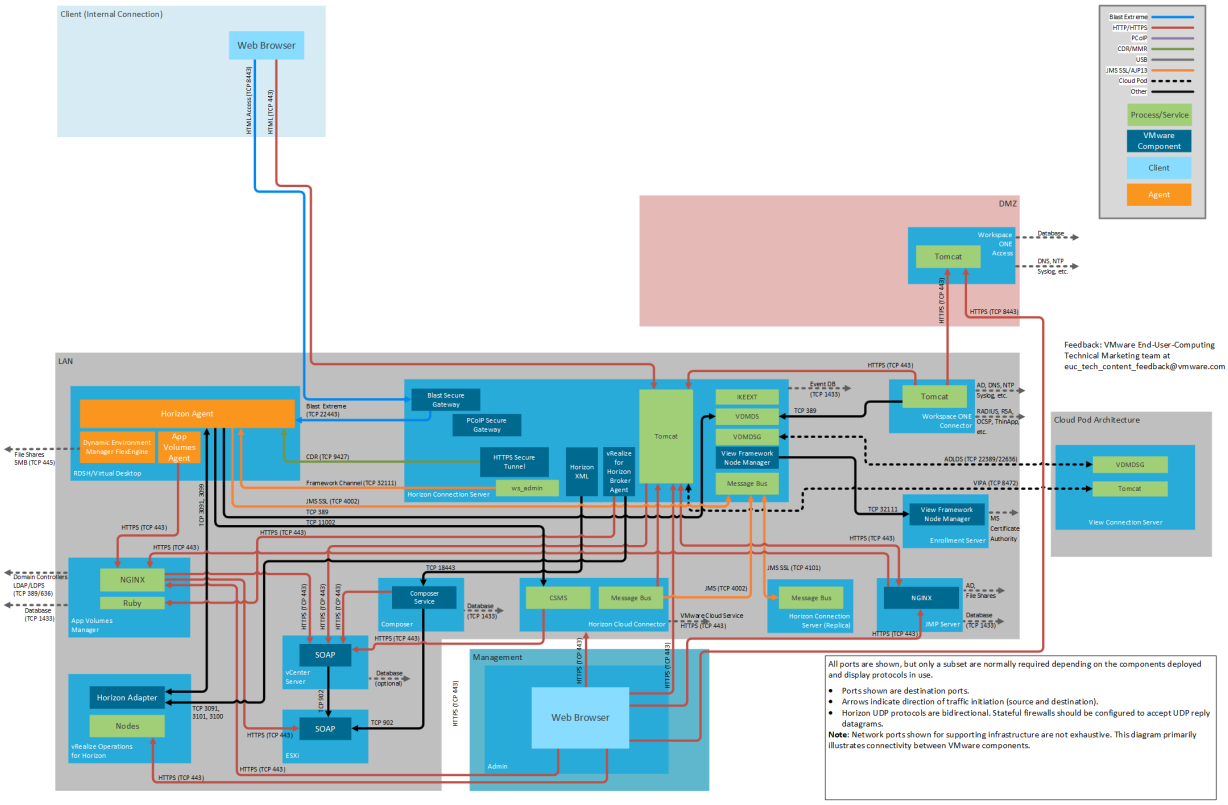
PCoIP Internal Connection



2021-06-28 Rev **Figure 4:** PCoIP

Internal Connection

HTML Access Internal Connection



2021-06-28 Rev **Figure 5:** HTML Access Internal Connection

External Connection

An external connection provides secure access into Horizon 7 resources from an external network. A Unified Access Gateway (UAG) or a security server (SS) provides the secure edge services. All communication from the client will be to that edge device, which then communicates to the internal resources.

The following table lists network ports for external connections from a client device to Horizon 7 components. The diagrams following the table show network ports for external connections, by display protocol, all with Unified Access Gateway.

Source	Destination	Network Protocol	Destination Port	Details
Horizon Client	Unified Access Gateway or security server	TCP	443	Login traffic. SSL (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in some cases. See *HTTP Redirection in Horizon 7* in Horizon 7 Security. Can also carry tunneled RDP, Client Drive Redirection, and USB redirection traffic.
		TCP	4172	PCoIP via PCoIP Secure Gateway on Unified Access Gateway or security server.
		UDP	4172	PCoIP via PCoIP Secure Gateway on Unified Access Gateway or security server.
	Unified Access Gateway	UDP	443	Optional for login traffic. Blast Extreme Blast Extreme tries a UDP login connection if the client experiences difficulty making a TCP connection to the UAG.
		TCP	8443	Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (performant channel).
		UDP	8443	Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic (adaptive transport).
		TCP	443	Blast Extreme via Blast Secure Gateway on Unified Access Gateway for data traffic where port sharing is used. This would be instead of TCP 8443.
	Security server	TCP	8443	Blast Extreme via Blast Secure Gateway on security server.
Browser	Unified Access Gateway or security server	TCP	8443 Or 443	Horizon 7 HTML Access. 8443 is the default but can be changed to 443 on Unified Access Gateway.
	Workspace ONE Access Appliance	TCP	443	Workspace ONE Access login and data traffic.
		Both	88	iOS (single-sign-on) SSO.
		TCP	5262	Android (single-sign-on) SSO.
		TCP	7443	SSL certificate authentication.
	Workspace ONE Access Connector	TCP	443	This port is only required for a connector being used in inbound mode. (outbound mode is recommended). If Kerberos authentication is configured on the connector, this port is required.

Notes:

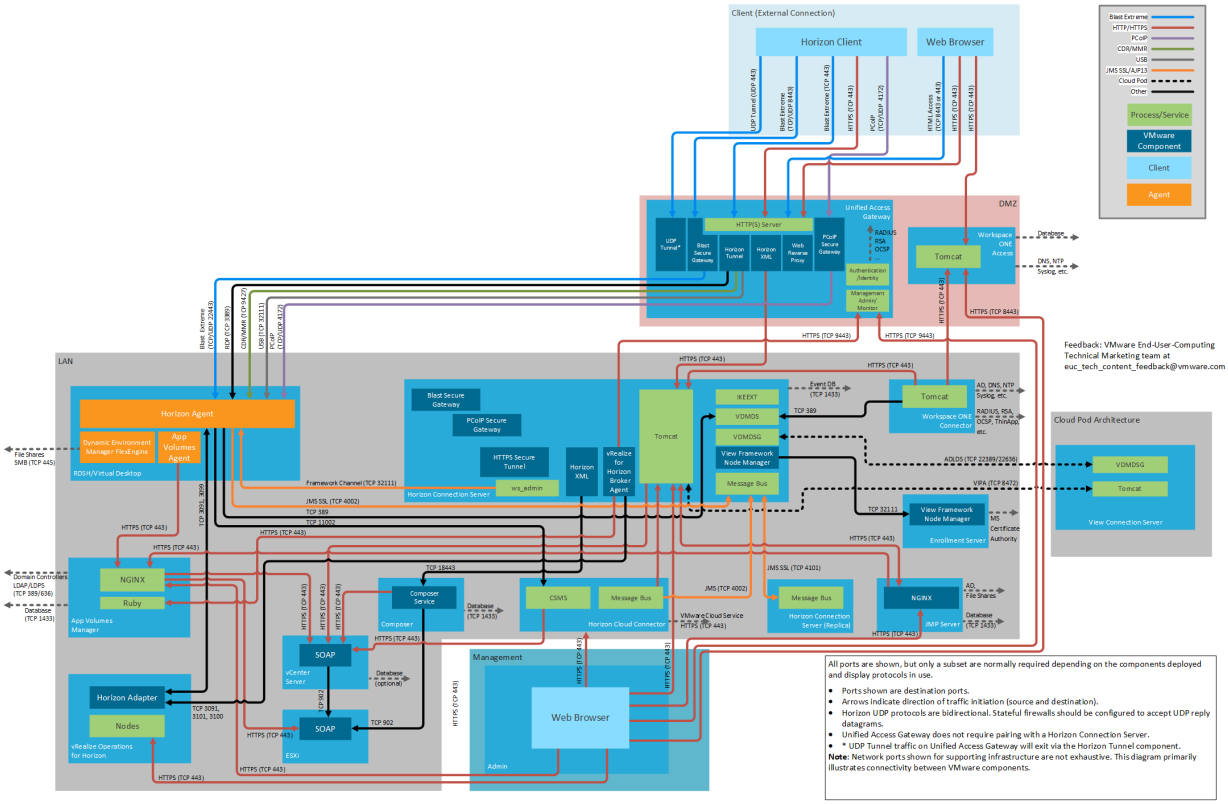
The Blast Secure Gateway on Unified Gateway can dynamically adjust to network conditions such as varying speeds and packet

loss. In Unified Access Gateway, you can configure the ports used by the Blast protocol.

- By default, Blast Extreme uses the standard ports TCP 8443 and UDP 8443.
- However, port 443 can also be configured for Blast TCP.
- The port configuration is set through the Unified Access Gateway Blast External URL property. See Blast TCP and UDP External URL Configuration Options.

If you configure Unified Access Gateway to use both IPv4 and IPv6 mode, then the Blast TCP/UDP must be set to port 443. You can enable Unified Access Gateway to act as a bridge for IPv6 Horizon clients to connect to an IPv4 backend Connection Server or agent environment. See Unified Access Gateway Support for IPv4 and IPv6 Dual Mode for Horizon Infrastructure.

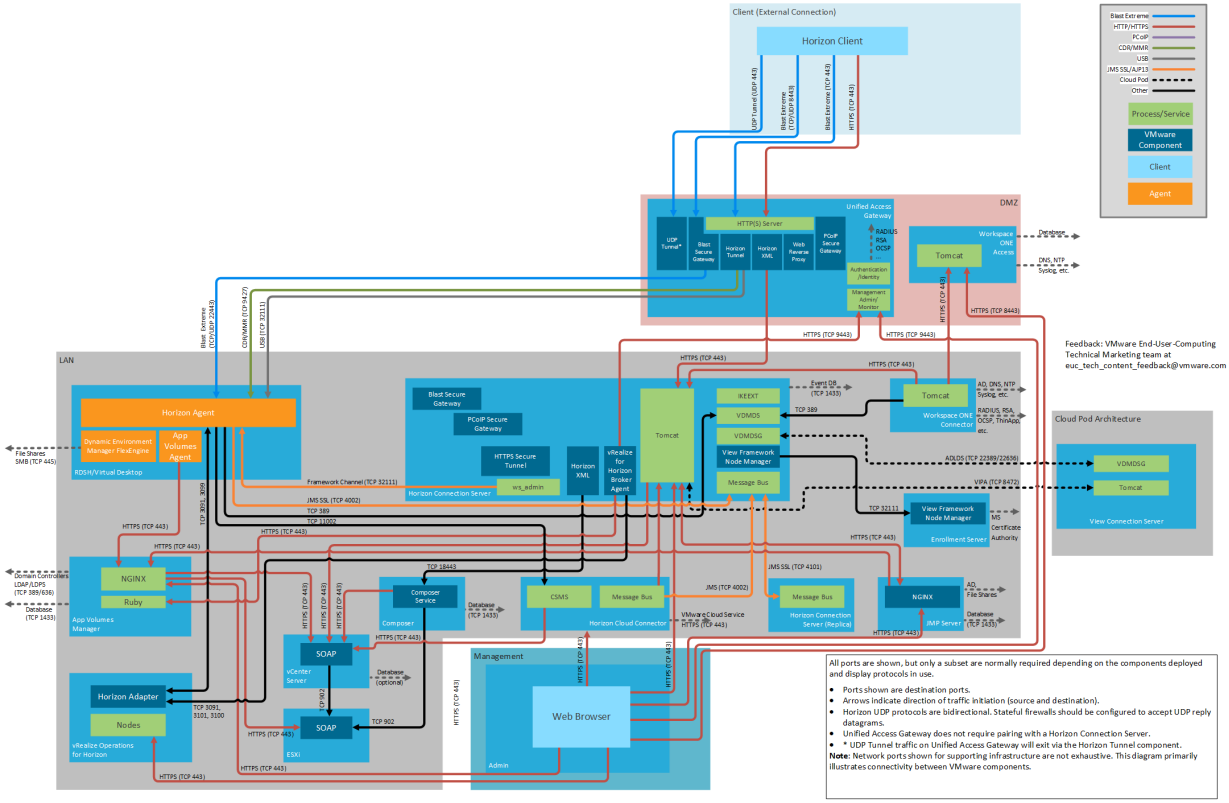
External Connection Showing All Display Protocols



2021-06-28 Rev **Figure 6:**

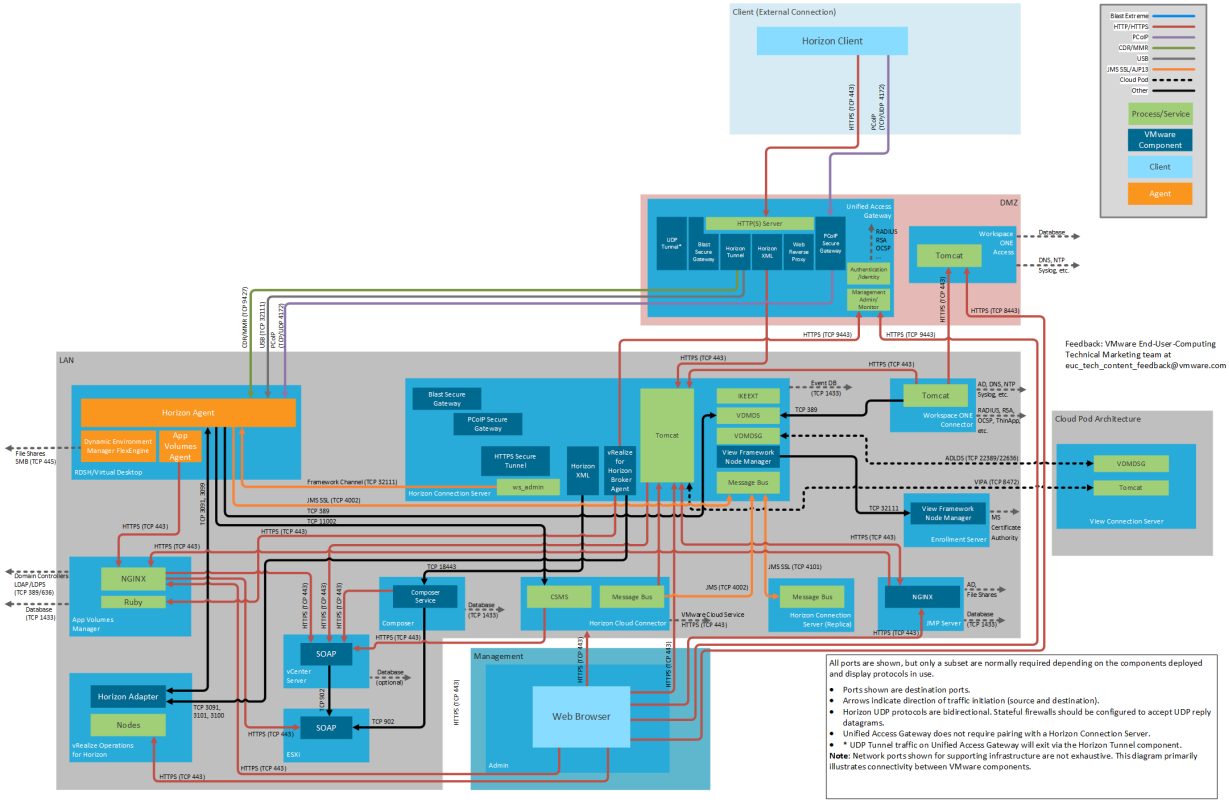
External Connection Showing All Display Protocols

Blast Extreme External Connection



2021-06-28 Rev **Figure 7:** Blast Extreme External Connection

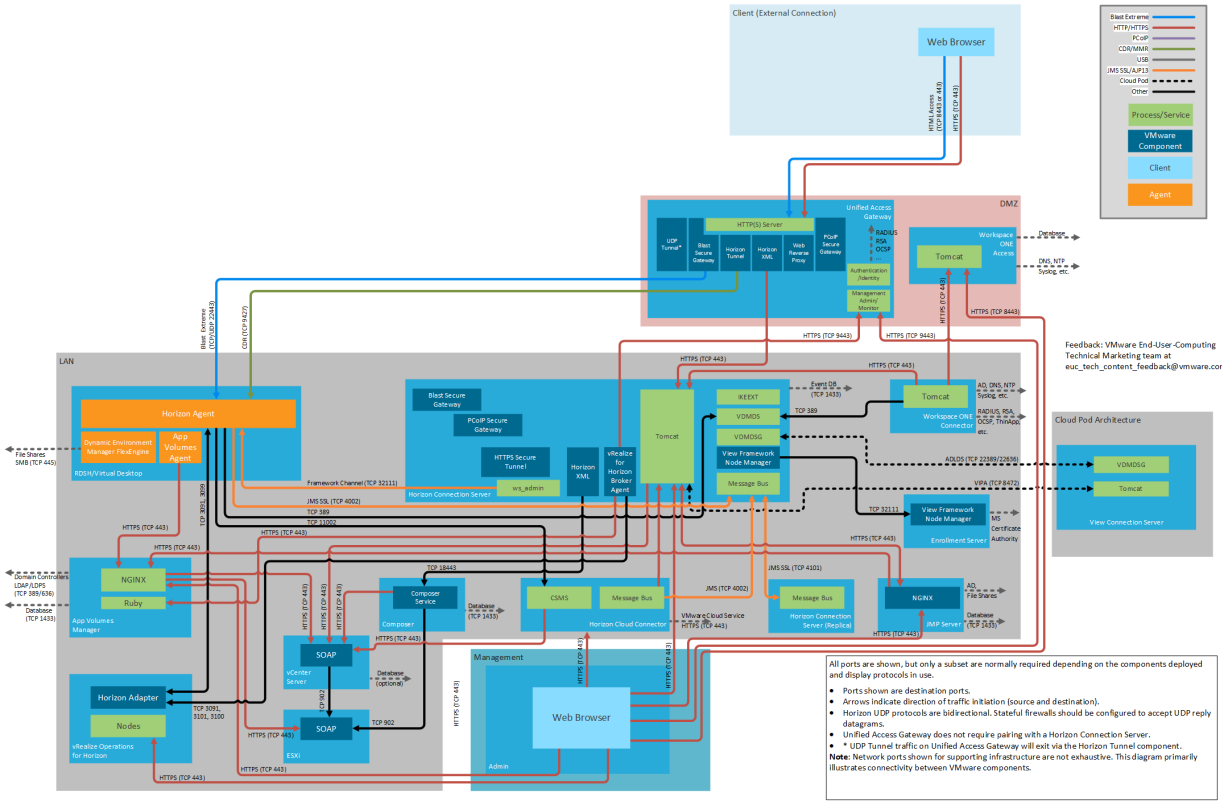
PCoIP External Connection



2021-06-28 Rev **Figure 8:** PCoIP

External Connection

HTML Access External Connection



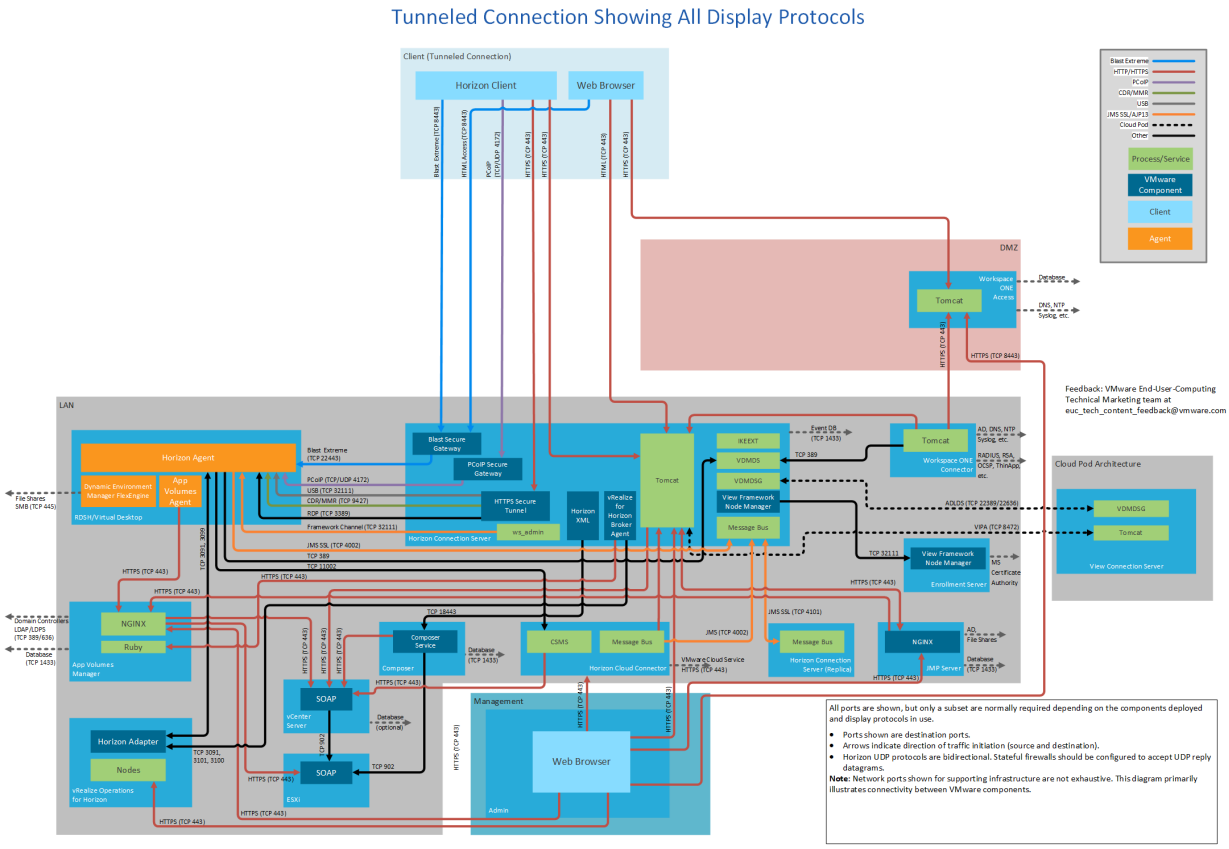
2021-06-28 Rev **Figure 9:** HTML Access External Connection

Tunneled Connection

A tunneled connection uses the Horizon Connection Server to provide gateway services. Authentication and session traffic is routed through the Horizon Connection Server. This approach is less frequently used because Unified Access Gateway can provide the same and more functionality.

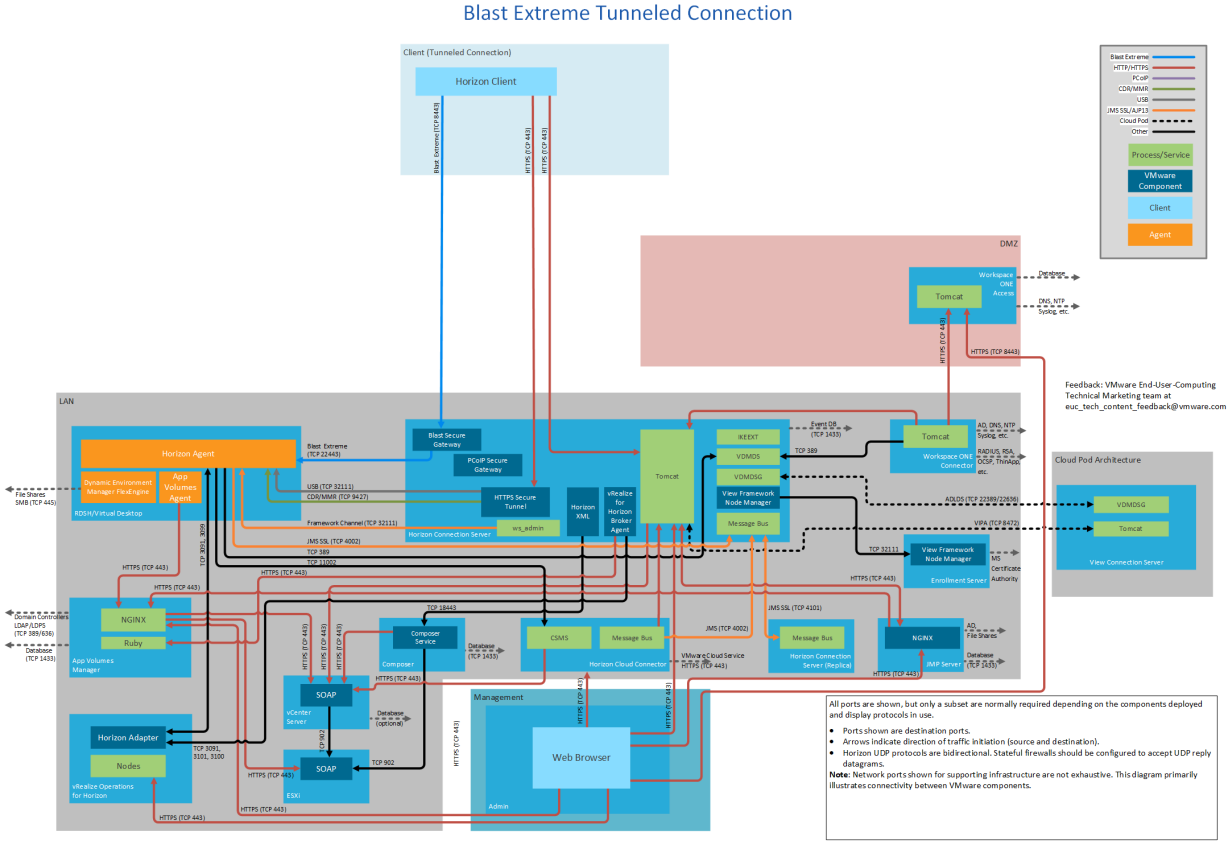
The following table lists network ports for tunneled connections from a client device to the Horizon 7 components. The diagrams following the table show network ports for tunneled connections, by display protocol.

Source	Destination	Network Protocol	Destination Port	Details
Horizon Client	Horizon Connection Server	TCP	443	Login. SSL (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in certain cases. See *HTTP Redirection in Horizon 7* in Horizon 7 Security. Can also carry tunneled RDP, Client Drive Redirection, and USB redirection traffic.
		TCP	8443	Blast Extreme to Blast Secure Gateway.
		TCP	4172	PCoIP to PCoIP Secure Gateway.
		UDP	4172	PCoIP to PCoIP Secure Gateway.
Browser	Horizon Connection Server	TCP	8443	Horizon 7 HTML Access.
	Workspace ONE Access Appliance	TCP	443	Workspace ONE Access login and data traffic.
		Both	88	iOS (single-sign-on) SSO.
		TCP	5262	Android (single-sign-on) SSO.
		TCP	7443	SSL certificate authentication.
	Workspace ONE Access Connector	TCP	443	This port is only required for a connector being used in inbound mode (outbound mode is recommended). If Kerberos authentication is configured on the connector, this port is required.



2021-06-28 Rev **Figure 10:**

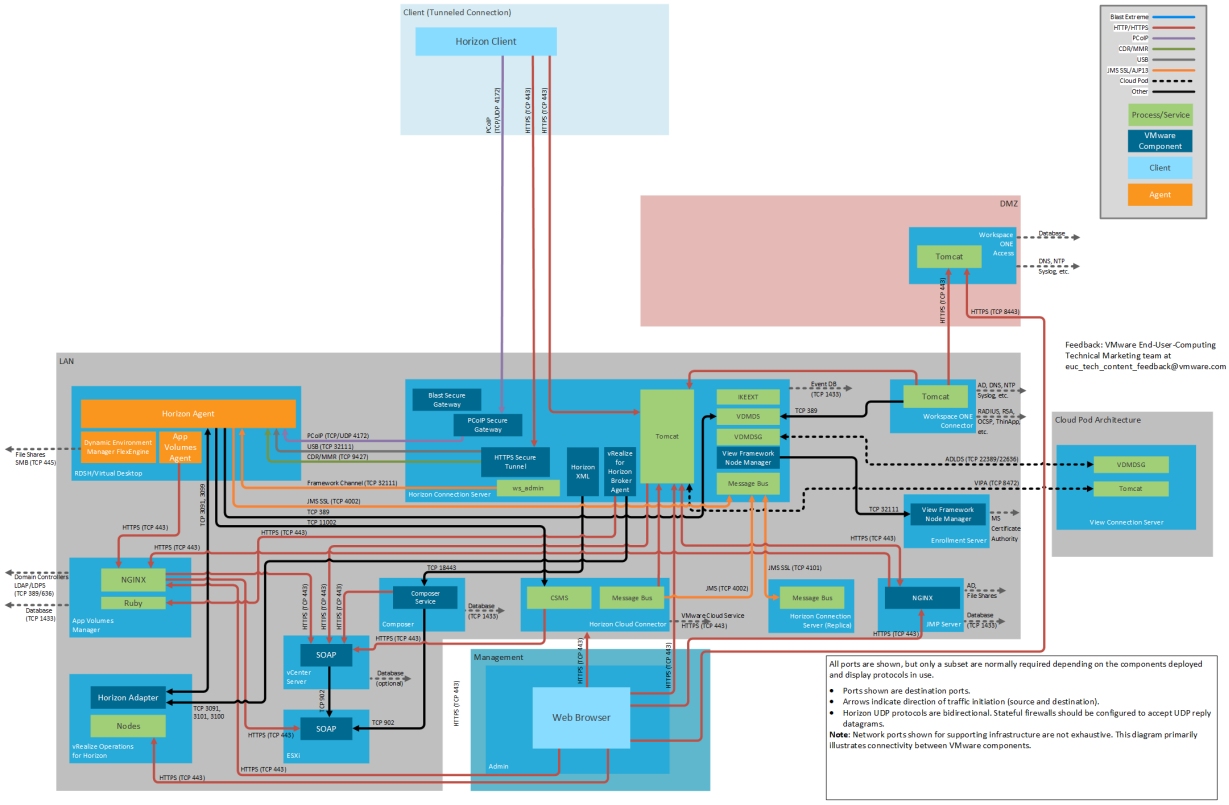
Tunneled Connection Showing All Display Protocols



2021-06-28 Rev **Figure 11:**

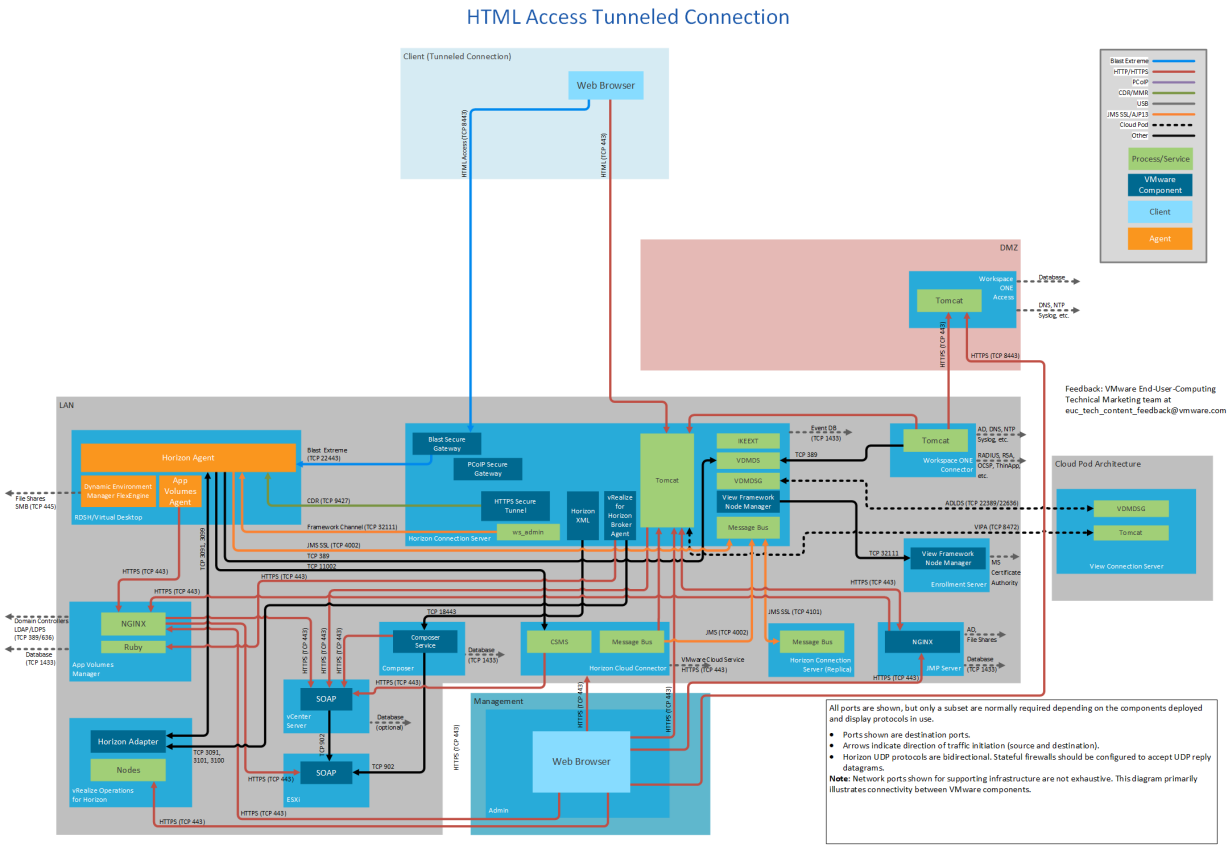
Blast Extreme Tunneled Connection

PCoIP Tunneled Connection



2021-06-28 Rev **Figure 12:**

PCoIP Tunneled Connection



2021-06-28 Rev **Figure 13:** HTML Access Tunneled Connection

Virtual Desktop or RDS Host

The following table lists network ports for connections from a virtual desktop or RDS host, to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
Horizon Agent	Horizon Connection Server	TCP	4001	Java Message Service (JMS).
		TCP	4002	Java Message Service (JMS) when using enhanced security (default).
		TCP	389	Only required when doing an unmanaged agent registration, for example, RDSH agent install without linked-clone or instant-clone component.
	Horizon Cloud Connector	TCP	11002	Agent data collection.
	vRealize Operations for Horizon *	TCP	3091	Remote Method Invocation (RMI) registry lookup.
		TCP	3099	Desktop message server.
App Volumes Agent	App Volumes Manager	TCP	443	Can use port 80 if not using SSL certificates to secure communication.
Dynamic Environment Manager FlexEngine	File shares	TCP	445	Dynamic Environment Manager agent access to SMB file shares.

* VMware vRealize Operations for Horizon ports shown are for version 6.2 and later. See the vRealize Operations for Horizon Documentation for earlier versions.

Horizon Connection Server

The following table lists network ports for connections from a Horizon Connection Server to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
Horizon Connection Server	Horizon Agent	TCP	22443	Blast Extreme for a tunneled connection.
		TCP	4172	PCoIP for a tunneled connection.
		UDP	4172	PCoIP for a tunneled connection.
		TCP	3389	RDP for a tunneled connection.
		TCP	9427	Optional for client drive redirection (CDR) and multi-media redirection (MMR) for a tunneled connection. By default, when using Blast Extreme, CDR traffic is side-channeled in the Blast Extreme ports indicated previously. If desired, this traffic can be separated onto the port indicated here.
		TCP	32111	Framework channel - used by ws_admin One use is for vdmadmin to configure or read from the agent. For example, creating a Data Collection Tool (DCT) log bundle. (vdmadmin -A -getDCT...)
		TCP	32111	Optional for USB redirection for a tunneled connection.
	vCenter Server	TCP	443	SOAP messages.
	Horizon Connection Server	TCP	4100	JMS to replica Horizon Connection Server for redundancy and scale.
		TCP	4101	JMS SSL to replica Horizon Connection Server for redundancy and scale.
		TCP	32111	Used during installation of a replica Horizon Connection Server and when rekeying the cluster master secret.
		TCP	135	MS-RPC endpoint mapper. Required for Connection Server replication.
		TCP	49152 -65535	MS-RPC dynamic client port range. Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Server instances. These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication. See note below.
		TCP	389	Only used during installation of a replica Horizon Connection Server.
		TCP	22389	Cloud Pod Architecture ADLDS – global LDAP replication.
		TCP	22636	Cloud Pod Architecture ADLDS – secure global LDAPS replication.
		TCP	8472	Cloud Pod Architecture inter-pod VIPA.
	Database (Events)	TCP	1433	If using a Microsoft SQL database (default port is 1443).
		TCP	1521	If using an Oracle database.
	Enrollment server	TCP	32111	Framework channel.
	JMP Server	TCP	443	
	View Composer	TCP	18443	SOAP messages.
	Security server	UDP	500	IPsec negotiation traffic.
		UDP	4500	NAT-T ISAKMP.
	Workspace ONE Access Appliance	TCP	443	Message bus.
	vRealize Operations for Horizon (V4H)	TCP	3091	Remote Method Invocation (RMI) registry lookup.
		TCP	3101	Broker message server – send topology data.
		TCP	3100	Certificate management server – pair.
	Unified Access Gateway	TCP	9443	vRealize Operations for Horizon broker agent monitoring of UAG appliances.
	App Volumes Manager	TCP	443	vRealize Operations for Horizon broker agent monitoring of App Volumes Managers.
	RSA SecurID Authentication Manager	UDP	5500	2-factor authentication. Default value is shown. This port is configurable.

Notes:

Replication requires RPC ports between Connection Servers, both within a Pod and between Pods with Cloud Pod Architecture (CPA). The RPC port numbers are dynamically allocated after initial communication with the RPC endpoint mapper over TCP port 135. For more information about the dynamic range of ports, see the Microsoft Windows Server documentation.

- Review the RPC port requirements for the different Microsoft Server OS versions: https://support.microsoft.com/en-gb/help/179442/how-to-configure-a-firewall-for-domains-and-trusts
- To understand RPC dynamic ports see: Active Directory and Active Directory Domain Services Port Requirements
- The ports required can be restricted: https://support.microsoft.com/en-gb/help/224196/restricting-active-directory-rpc-traffic-to-a-specific-port

Unified Access Gateway

The following table lists network ports for connections from a Unified Access Gateway to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
Unified Access Gateway	Horizon Connection Server	TCP	443	Login.
	Horizon Agent	TCP	22443	Blast Extreme.
		UDP	22443	Blast Extreme.
		TCP	4172	PCoIP.
		UDP	4172	PCoIP.
		TCP	3389	RDP.
		TCP	9427	Windows multimedia redirection, client drive redirection, HTML5 multimedia redirection, Microsoft Teams optimization, VMware printer redirection, and USB redirection. By default, when using Blast Extreme, CDR traffic is side-channeled in the Blast Extreme ports indicated previously.
		TCP	32111	Optional for USB redirection. USB traffic can also be side-channeled in the Blast Extreme ports indicated previously. See note below.
	RADIUS,...	UDP	5500	Other authentication sources such as RADIUS. Default value for RADIUS is shown but is configurable.

Notes:

With the VMware Blast display protocol, you can configure USB features, such as USB redirection, and client drive redirection, to send side channel traffic over a Blast Extreme ports. See:

- Enabling the USB Over Session Enhancement SDK Feature.
- Managing Access to Client Drive Redirection.

Enrollment Server

The following table lists network ports for connections from a Horizon Enrollment Server.

Source	Destination	Network Protocol	Destination Port	Details
Enrollment Server	AD Certificate Services	TCP	135	Enrollment Server requests certificate from Microsoft Certificate Authority (CA) to generate a temporary, short-lived certificate. The enrollment service uses TCP 135 RPC for the initial communication with the CA, then a random port from 1024 - 5000 and 49152 -65535. See Certificate Services in https://support.microsoft.com/en-us/help/832017#method4.
	AD Domain Controllers			Enrollment Server also communicates with domain controllers, using all relevant ports to discover a DC and bind to and query the Active Directory. See https://support.microsoft.com/en-us/help/832017#method1 and https://support.microsoft.com/en-us/help/832017#method12.

Horizon Cloud Connector

The Horizon Cloud Connector is a virtual appliance that connects a Connection Server in a pod with the VMware Cloud Service. The Horizon Cloud Connector is required when using Horizon 7 subscription licenses and Horizon Cloud Services. The following table lists network ports for connections from a Horizon Cloud Connector.

Source	Destination	Network Protocol	Destination Port	Details
Horizon Cloud Connector	Horizon Connection Server	TCP	443	Horizon pod integration.
		TCP	4002	Java Message Service (JMS).
	vCenter Server	TCP	443	Used by the Image Management Service (IMS). Used during automatic upgrade of connector.
	VMware Cloud Service Control Plane	TCP	443	Regional control plane instance. https://cloud.horizon.vmware.com Plus, one of the following names, depending on which regional control plane instance is specified in your Horizon Cloud tenant account. • cloud-us-2.horizon.vmware.com • cloud-eu-central-1.horizon.vmware.com • cloud-eu-2.horizon.vmware.com • cloud-ap-southeast-2.horizon.vmware.com • cloud-ap-2.horizon.vmware.com • cloud-jp.horizon.vmware.com • cloud-uk.horizon.vmware.com
	Horizon Cloud Monitoring Service (CMS)	TCP	443	Depends on which regional control plane is specified in your Horizon Cloud account. North America: • kinesis.us-east-1.amazonaws.com • query-prod-us-east-1.cms.vmware.com Europe: • kinesis.eu-central-1.amazonaws.com • query-prod-eu-central-1.cms.vmware.com Australia: • kinesis.ap-southeast-2.amazonaws.com • query-prod-ap-southeast-2.cms.vmware.com Japan: • kinesis.ap-northeast-1.amazonaws.com • query-prod-ap-northeast-1.cms.vmware.com United Kingdom: • kinesis.eu-west-2.amazonaws.com • query-prod-eu-west-2.cms.vmware.com
	Certificate Authority	TCP	443	CRL or OCSP queries CRL used to obtain validation from the certificate authority, DigiCert *.digicert.com
	Universal Broker	TCP	443	Regional instance of the Universal Broker service depending on which regional control plane instance is specified in your Horizon Cloud tenant account. United States: • connector-azure-us.vmwarehorizon.com Europe: • connector-azure-eu.vmwarehorizon.com Australia: • connector-azure-aus.vmwarehorizon.com Japan: • connector-azure-jp.vmwarehorizon.com United Kingdom: • connector-azure-uk.vmwarehorizon.com Germany: • connector-azure-de.vmwarehorizon.com
	Horizon Cloud Connector	TCP	22	Used during upgrades. Listen for requests to start the upgrade process.

Notes:

The regional instance is set when the account is created, as described in Deployments and Onboarding to Horizon Cloud for Microsoft Azure and Horizon Pods.

Certificate Authority - If your organization discourages the use of wildcards in allowable DNS names, you can specify specific names to DigiCert for the Certificate Authority CRL or OCSP queries. At the time of this writing, the specific DNS names required for certificate validation are:

- ocsp.digicert.com

- crl3.digicert.com
- crl4.digicert.com
- www.digicert.com/CPS

These DNS names are determined by DigiCert and subject to change. For instructions on how to obtain the specific names required by your certificates, refer to VMware Knowledge Base (KB) article 79859.

vCenter Server and View Composer

The following table lists network ports for connections from a vCenter Server and a View Composer server, to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
vCenter Server	ESXi	TCP	902	SOAP.
View Composer	vCenter Server	TCP	443	SOAP.
	ESXi	TCP	902	SOAP.
	Database	TCP	1433	If using a Microsoft SQL database (default port is 1443).
		TCP	1521	If using an Oracle database.

JMP Server

The following table lists network ports for connections from a JMP Server, to other Horizon 7 components.

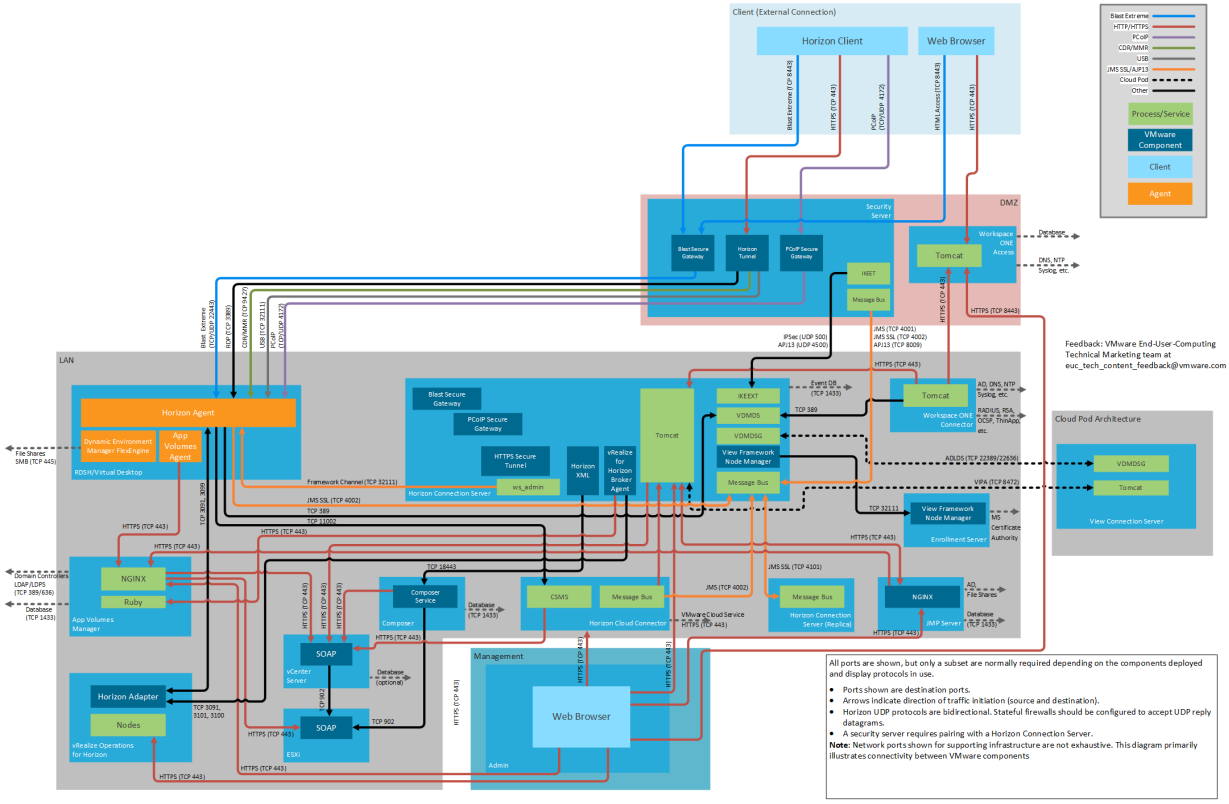
Source	Destination	Network Protocol	Destination Port	Details
JMP Server	Database	TCP	1433	Microsoft SQL database (default port is 1443).
	Horizon Connection Server	TCP	443	
	Active Directory	TCP	389	LDAP (non-secure) or LDAP over TLS. (AD ports can be customized)
		TCP	636	LDAPS
	App Volumes Manager	TCP	443	
	Dynamic Environment Manager file shares.	Both	135-139	Microsoft file sharing SMB: User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).
		Both	445	Direct-hosted SMB traffic without NetBIOS.

Security Server

The following table lists network ports for connections from a Horizon 7 security server to other Horizon 7 components. The diagrams following the table show network ports for external connections when using a security server, by display protocol.

Source	Destination	Network Protocol	Destination Port	Details
Security server	Horizon Connection Server	UDP	500	IPsec negotiation traffic.
		ESP		IP Protocol 50. AJP13-forwarded web traffic, when using IPsec without a NAT device.
		UDP	4500	AJP13-forwarded web traffic, when using IPsec through a NAT device.
		TCP	8009	AJP13-forwarded web traffic, if not using IPsec.
		TCP	4001	Java Message Service (JMS).
		TCP	4002	Java Message Service (JMS) when using enhanced security (default).
	Horizon Agent	TCP	22443	Blast Extreme.
		TCP	4172	PCoIP.
		UDP	4172	PCoIP.
		TCP	3389	RDP.
		TCP	9427	Optional for client drive redirection (MMR) and multi-media redirection (MMR). By default, when using Blast Extreme, CDR traffic is side-channeled in the Blast Extreme ports indicated above. If you prefer, this traffic can be separated onto the port indicated here.
		TCP	32111	Optional for USB redirection. By default, USB traffic is side-channeled in the Blast Extreme or PCoIP ports indicated previously. If you prefer, this traffic can be separated onto the port indicated here.

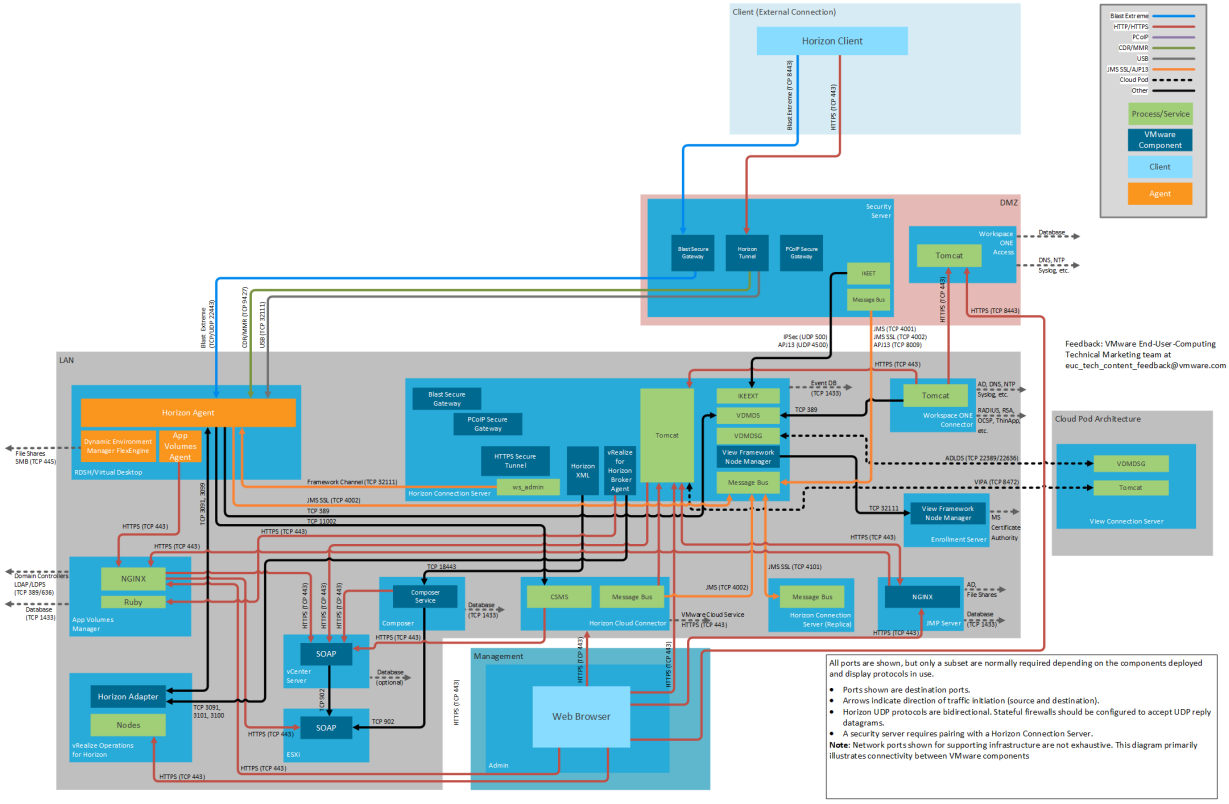
External Connection Showing All Display Protocols (Using Security Server)



2021-06-28 Rev **Figure 14:**

External Connection Showing All Display Protocols (Using Security Server)

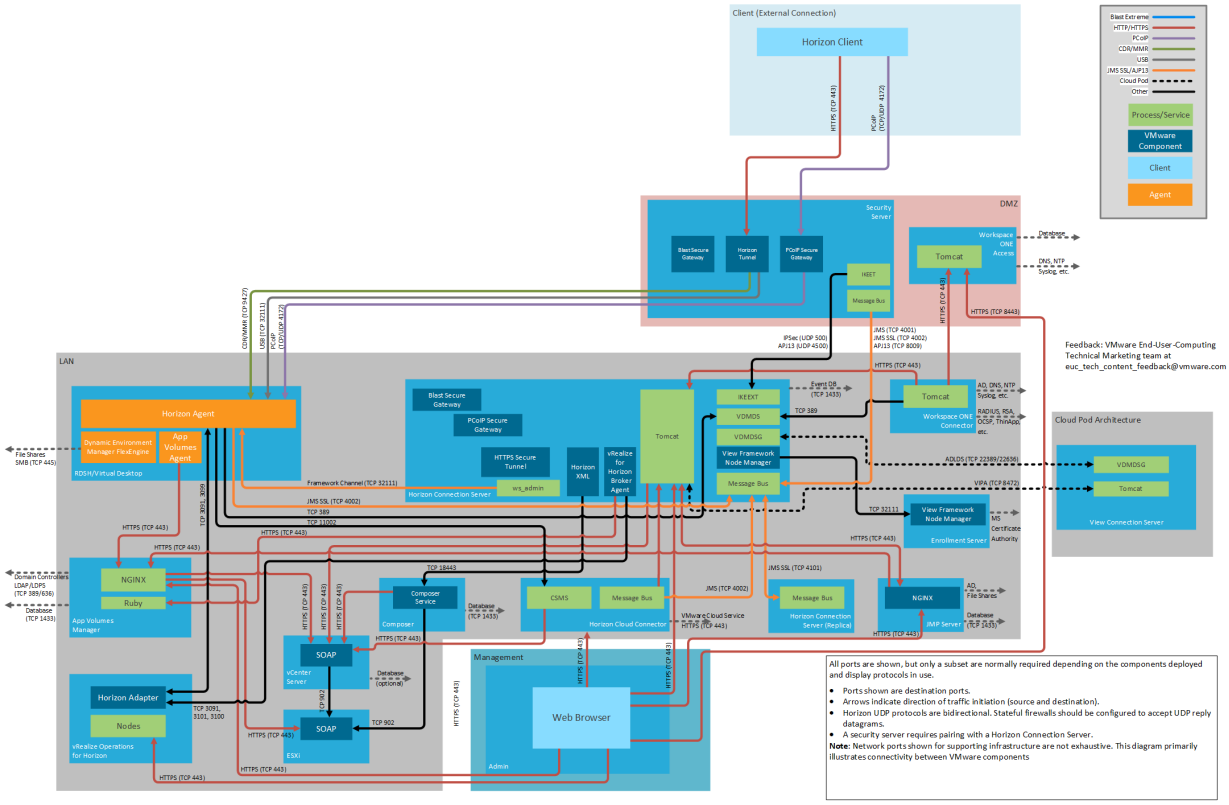
Blast Extreme External Connection (Using Security Server)



2021-06-28 Rev **Figure 15:**

Blast Extreme External Connection (Using Security Server)

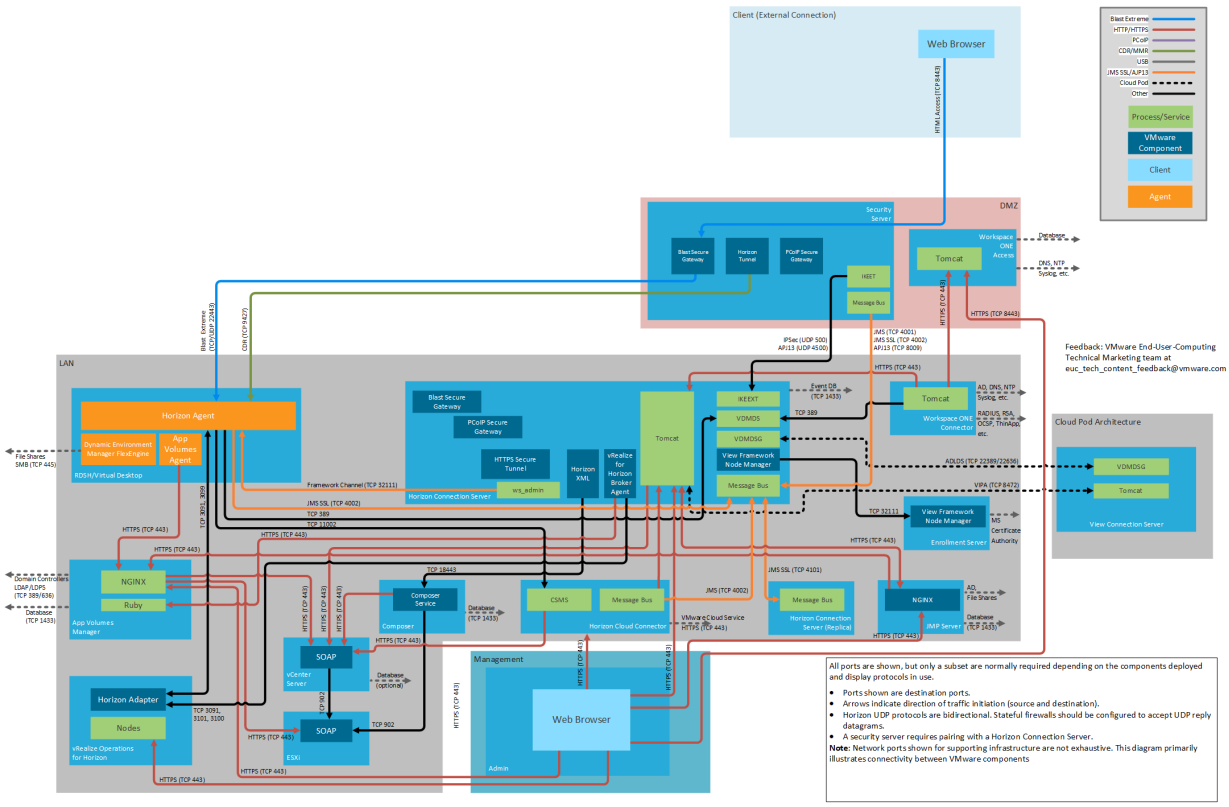
PCoIP External Connection (Using Security Server)



2021-06-28 Rev **Figure 16:**

PCoIP External Connection (Using Security Server)

HTML Access External Connection (Using Security Server)



2021-06-28 Rev **Figure 17:** HTML Access External Connection (Using Security Server)

Workspace ONE Access

The following table lists the network ports for connections from Workspace ONE Access (formerly VMware Identity Manager) to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
Workspace ONE Access Appliance	Workspace ONE Access Appliance	TCP	443	Appliance to appliance cluster communication
		TCP	8443	Appliance to appliance cluster communication
		TCP	8200	ElasticSearch.
		TCP	5701	Hazelcast cache.
		TCP	40002 40003	EHCache.
		TCP	9300	Audit needs.
		UDP	54328	Audit needs.
		TCP	9400	vPostgres.
	DNS servers	Both	53	DNS Lookup.
	NTP	UDP	123	Time sync.
	SMTP server	TCP	25	SMTP port to relay outbound mail.
	Syslog	UDP	514	For external syslog server, if configured.
	Log Insight	TCP	9543	
	OCSP	TCP	80	Online Certificate Status Protocol.
	KDC	UDP	88	Hybrid KDC.
	VMware Verify	TCP	443	
	Database	TCP	1433	If using an external Microsoft SQL database (default port is 1443).
		TCP	5432	If using an external PostgreSQL database.
		TCP	1521	If using an external Oracle database.
	Workspace ONE UEM (AirWatch) REST API	TCP	443	For device compliance-checking, and for the AirWatch Cloud Connector password authentication method, if that is used.
	vapp-updates.vmware.com	TCP	443	Access to the upgrade server.

Source	Destination	Network Protocol	Destination Port	Details
Workspace ONE Access Connector	Workspace ONE Access Appliance	TCP	443	Connector to appliance communication.
	Horizon Connection Server	TCP	443	Horizon 7 integration.
		TCP	389	Communication to Lightweight Directory Services (LDS) to sync entitlements.
	Domain controllers	TCP	389	LDAP to Active Directory. Default, but is configurable.
		TCP	636	LDAPS to Active Directory.
		TCP	3268	AD Global Catalog.
		TCP	3269	AD Global Catalog.
		Both	88	Kerberos authentication.
		Both	464	Kerberos password change.
		TCP	135	RPC.
	DNS servers	Both	53	DNS Lookup.
	NTP	UDP	123	Time sync.
	Syslog	UDP	514	
	Log Insight	TCP	9543	
	OCSP	TCP	80	Online Certificate Status Protocol.
	File servers	TCP	445	Access to the ThinApp repository on SMB share.
	RADIUS Server	TCP	1812	
		TCP	1813	
	RSA SecurID system	TCP	5500	Default value is shown. This port is configurable.
	Citrix Integration Broker server	TCP	80, 443	Connection to the Citrix Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server.
	vapp-updates.vmware.com	TCP	443	Access to the upgrade server.

App Volumes Manager

The following table lists network ports for connections from App Volumes Manager to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
App Volumes Manager	App Volumes Manager	TCP	3001	HTTP
		TCP	3002	HTTP
		TCP	3003	HTTP
		TCP	3004	HTTP
		TCP	54311	HTTPS
	vCenter Server	TCP	443	SOAP.
	ESXi	TCP	443	Hostd.
	Database	TCP	1433	Default port for Microsoft SQL.
	Active Directory	TCP	389	LDAP
		TCP	636	LDAPS (Optional)

vRealize Operations for Horizon

The following table lists network ports for connections from vRealize Operations for Horizon, to other Horizon 7 components.

Source	Destination	Network Protocol	Destination Port	Details
vRealize Operations for Horizon	Horizon Connection Server	TCP	3091	Remote Method Invocation (RMI) registry lookup.
		TCP	3101	Broker message server – send topology data.
		TCP	3100	Certificate management server – pair.
	Horizon Agent	TCP	3091	Remote Method Invocation (RMI) registry lookup.
		TCP	3099	Desktop message server.

Management

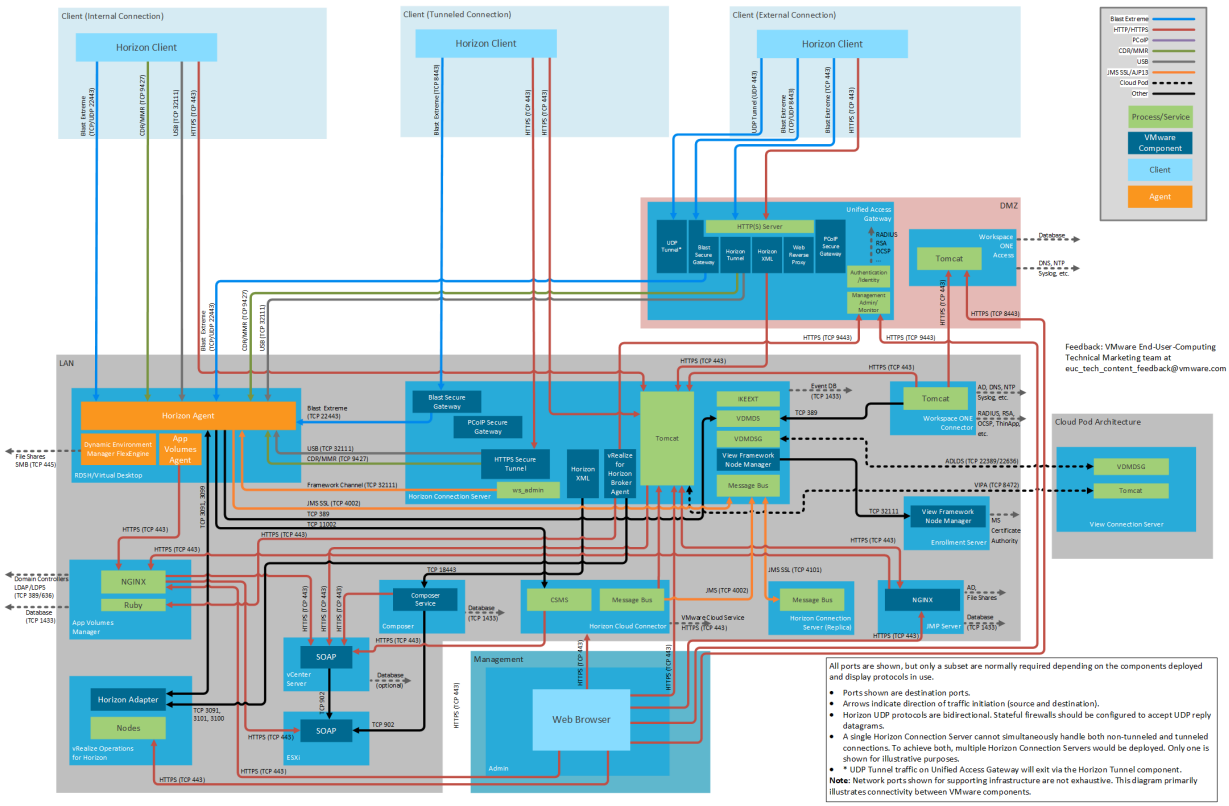
The following table lists network ports for the administrative consoles used in Horizon 7 Enterprise Edition.

Source	Destination	Network Protocol	Destination Port	Details
Admin browser	Horizon Connection Server	TCP	443	https://<Connection Server FQDN>/admin https://<Connection Server FQDN>/newadmin
	JMP Server	TCP	443	
	vCenter Server	TCP	443	https:// <vCenter Server FQDN>/
	Horizon Cloud Connector	TCP	443	
	App Volumes Manager	TCP	443	https:// <App Volumes Manager Server FQDN>/
	Workspace ONE Access Appliance	TCP	443	https://<W1 Access Instance FQDN>
		TCP	8443	https://<W1 Access Appliance FQDN>:8443/cfg/login
		TCP	22	SSH
	Workspace ONE Access Connector	TCP	8443	
		TCP	22	SSH
	vRealize Operations for Horizon	TCP	443	https://<vRealize Manager FQDN or IP Address>/admin
	Unified Access Gateway	TCP	9443	https://<UAG FQDN or IP Address>:9443/admin/

Display Protocol-Specific Diagram Views

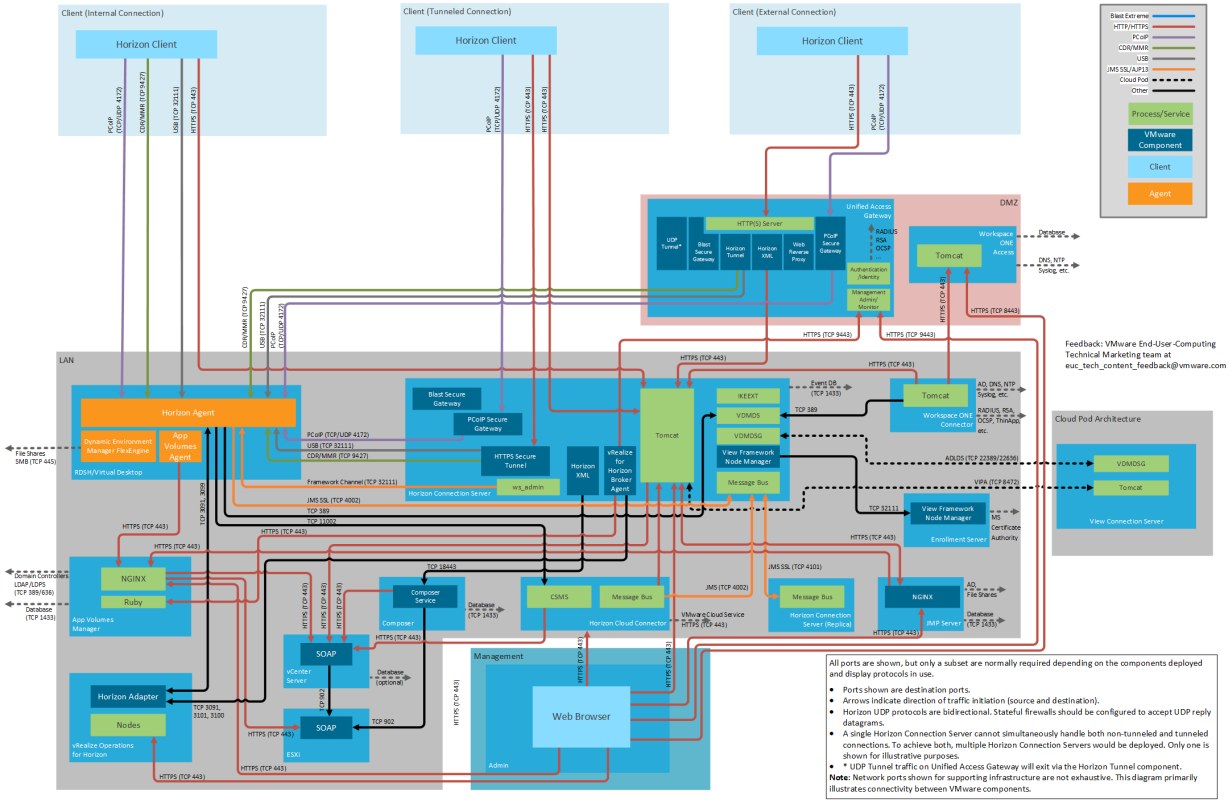
The following diagrams display network ports for connections, by display protocol (Blast Extreme or PCoIP), and for HTML Access client connections.

Blast Extreme Connections



2021-06-28 Rev Figure 18: Blast Extreme Connections

PCoIP Connections



2021-06-28 Rev **Figure 19:**

PCoIP Connections

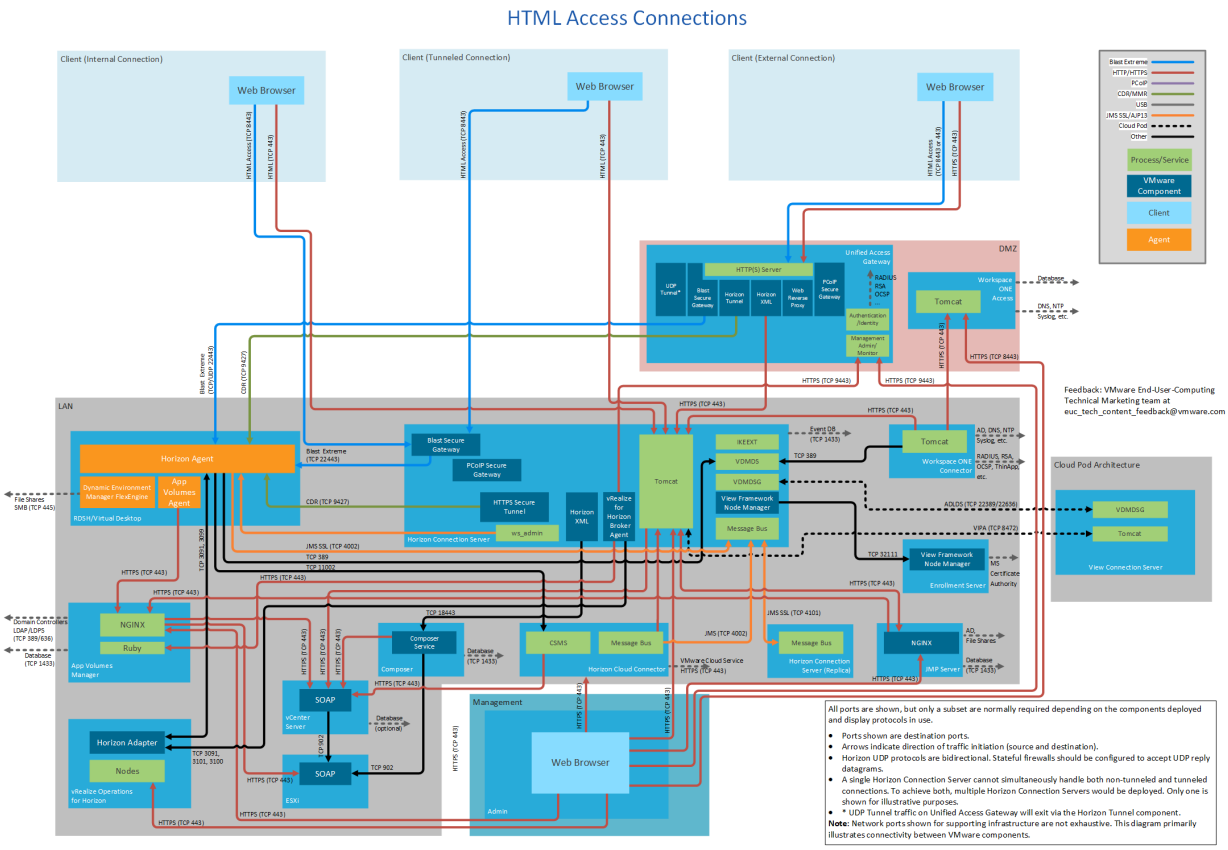


Figure 20: HTML Access Connections

Summary and Additional Resources

Additional Resources

For Horizon 8, see Network Ports in VMware Horizon.

Changelog

The following updates were made to this guide.

Date	Changes
2021-06-28	Diagrams updated to add in connection from Horizon Cloud Connector to vCenter Server.
2021-06-25	Additional port information for Horizon Cloud Connector added to cover the new services. Updated the information on the services that use ports TCP 4927 and 32111 from the Client (Internal Connection) and Unified Access Gateway.
2021-05-17	Additional port information for the Horizon Cloud Connector required for various control plane services. • vCenter Server for Image Management Service • Horizon Cloud Service Control Plane • Horizon Cloud Monitoring Service (CMS) URLs • Certificate Authority URLs • Universal Broker URLs Update links to Horizon 7.13 and Unified Access Gateway 2103 documentation.
2021-05-12	Removed the word legacy from JMS TCP 4001 as this described this incorrectly.
2020-05-28	Added new port information to document and diagrams for Horizon Cloud Connector. • Additional port information from Horizon Cloud Connector • Port from Horizon Agent to Horizon Cloud Connector Removed an old port (listed as PowerShell) between the App Volumes Agent and Managers which is no longer used. Reorganized diagrams to make them more readable.
2020-04-27	Corrected typo on App Volumes port from agent to manager for PowerShell.
2020-03-25	Update links to Horizon 7.12 and Unified Access Gateway 3.9 documentation. Added a note to the relevant diagrams to indicate that Horizon UDP traffic will enter the Unified Access Gateway by the UDP Tunnel and will exit via the Horizon Tunnel.
2019-09-18	Rename of VMware Identity Manager to VMware Workspace ONE Access. vRealize Operations for Horizon (V4H) – Added V4H broker agent to the Horizon Connection Server. Corrected ports and where they come from for V4H monitoring of Unified Access Gateways and App Volumes Managers.
2018-06-29	The default behavior for USB redirection had changed so updated the language in the Internal Connection and Unified Access Gateway tables to reflect this. Changed language on RPC ports in the Horizon Connection Server table to reflect that this applies to all Connection Server to Connection Server replication and not just CPA.

About the Author and Contributors

Graeme Gordon, Senior Staff End-User-Computing Architect, EUC Technical Marketing, VMware, wrote this document and created the accompanying network-port diagrams.

The following people contributed their knowledge and assisted with reviewing:

- Mark Benson, Senior Staff Engineer, EUC CTO Office, VMware
- Paul Green, Staff Engineer, Virtual Workspace R&D, VMware
- Ramu Panayappan, Director, Virtual Workspace R&D, VMware
- Mike Oliver, Staff Engineer, Virtual Workspace R&D, VMware
- Andrew Jewitt, Staff Engineer, Virtual Workspace R&D, VMware
- Rick Terlep, Senior EUC Architect, EUC Technical Marketing, VMware
- Jim Yanik, Senior Manager, EUC Technical Marketing, VMware
- Frank Anderson, VMware Alumni

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

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