Security Considerations for VMware® Horizon View™ 5.2

WHITE PAPER
Table of Contents

Overview ................................................................................................................. 3
Internal Deployment ............................................................................................. 3
  View Client and Endpoints .................................................................................. 5
  View Agent ........................................................................................................... 5
  Horizon View Desktops ........................................................................................ 6
  SSL Certificates ................................................................................................... 6
  Load Balancing Configuration .............................................................................. 7
  Antivirus and Antimalware ................................................................................... 8
  Integrating Horizon View into Active Directory ................................................. 8
External Deployment ............................................................................................. 9
  Security Server Considerations .......................................................................... 10
  Firewall and DMZ Configuration ......................................................................... 11
  Two-Factor Authentication ................................................................................... 12
    SecurID ............................................................................................................... 12
    RADIUS ............................................................................................................ 13
    PCoIP ................................................................................................................... 14
  Using vCloud Networking and Security to Secure the Horizon View Environment ... 14
    Sample Automobile Manufacturer Use Case Scenario ..................................... 15
  Monitoring the Horizon View Environment ....................................................... 16
Conclusion ............................................................................................................. 16
References ............................................................................................................. 17
About the Author .................................................................................................... 17
Overview

A VMware® Horizon View™ deployment on the VMware vSphere® product offers many options for securing virtual desktops. End users can access their desktops from supported Web browsers, laptops, and a range of other devices, including Apple and Android devices, inside or outside the corporate firewall, while corporate data and resources remain protected within the virtual datacenter.

A Horizon View deployment also provides a great deal of flexibility. For example, when accessing their virtual desktops, end users can redirect multimedia and USB devices for use within their Horizon View desktops as well as maintain personal profiles, which enable them to customize and maintain their desktop’s look and feel. With a personal profile, a user can also check a virtual desktop out to a local device, whether Bring Your Own Device (BYOD) or corporate-issued, and continue to work while mobile.

Because of this flexibility, you must exercise vigilance in order to keep access to user data both secure and unimpeded. As a safeguard against loss or theft, for instance, you can set controls to disable a device in local mode if it is not synchronized within a certain time interval. Hackers and other potential intruders are always exploring new ways to circumvent the security process.

This document describes the security options to consider when deploying Horizon View. It is divided into major sections on Internal Deployment and External Deployment.

• **Internal Deployment** describes the components that are deployed and the options for securing them when you deploy Horizon View inside the corporate network, including the View Agent, clients, and endpoints; SSL certificates; load balancing; antivirus and antimalware; and Active Directory (AD) integration.

• **External Deployment** includes discussions of security options for remote access from untrusted networks such as the Internet as well as firewalls, and enhanced security options such as two-factor authentication using RADIUS and RSA SecurID.

Internal Deployment

When you configure VMware Horizon View for internal use, you deploy the VMware View Composer™ Server and the View Connection Server(s). These servers are joined to an Active Directory domain and are subject to all the polices implemented by Group Policy for that domain. You can implement additional policies with the Horizon View Group Policy Administrative (ADM) Template files, which extend the Active Directory Group Policy. ADM Template files enable:

• **View Agent configuration** – View Agent settings for authentication and environment control
• **View Client configuration** – View Client settings for connection and other configuration policies
• **View PCoIP session** – View policy that controls configuration of the PCoIP display protocol
• **View Persona Management** – View policy settings that control user profiles
• **View common configuration** – View policy settings that are common to all View components
• **View Server configuration** – View policy settings that allow additional configuration of the View Connection Server
You can also enhance the security of a Horizon View environment by enabling or disabling the following capabilities:

- Connection to the Horizon View environment when certificates have expired
- Single sign-on
- Use of command-line credentials
- Login as current user

Before planning for remote access to the Horizon View internal deployment, implement the Group Policy and Horizon View extended policies best suited to your organization on the Organizational Units (OUs) that you create for your users and desktops. Horizon View is integrated with Active Directory and subject to its security policy, so begin by securing Horizon View with AD Group Policy, then use Horizon View extended policies for further enhancement.

**Note:** Consider the policy settings for the Horizon View deployment carefully to make sure that they do not cause end-user productivity to be degraded.

Figure 1 illustrates an internal Horizon View deployment. In a simple Horizon View environment, a single View Connection Server can be deployed to support up to 2000 simultaneous connections on the internal network, even without the use of a load balancer. The configuration in this figure, however, includes load balancing.

![Figure 1: Internal Deployment with Load Balancing](image)

**Note:** In an external Horizon View deployment, designed to enable remote access, the load balancing function is moved into the demilitarized zone (DMZ) to load balance remote users across View Security Servers, as shown in Figure 3 (see Load Balancing Configuration).
View Client and Endpoints

The Horizon View Client Configuration ADM template provides security-specific settings for secure Horizon View access. Consider implementing some of the following settings:

- **Allow command line credentials** - Determines whether users can use the command line to enter their credentials.

- **Servers Trusted For Delegation** - Specifies the View Connection Server instances that accept the user identity and credentials information that is passed when a user selects the **Log in as current user** check box.

- **Certificate verification mode** - Configures the level of certificate checking performed by the View Client.

- **Enable Single Sign-On for smart card authentication** - Determines whether single sign-on is enabled for smart card authentication.

For more information on these security settings, see *VMware Horizon View Administration* and *VMware Horizon View Security*.

For devices serving as Horizon View endpoints, verify that the operating systems, if any, employ the latest security patches and follow all vendor rules for securing the operating system to reduce the attack surface. If possible, employ the hardware-based security capabilities for the endpoint device, such as the Trusted Platform Module (TPM). Most modern devices use the TPM as an added means for providing user identity and security for laptop devices. Since each device has an RSA key burned in when it is produced, it can perform platform authentication in the event it is lost or stolen. This can render a lost or stolen laptop or other TPM-capable device useless by preventing it from booting the operating system. Other BIOS options include hard disk encryption and a hardware password to prevent access or tampering with the hardware.

Verify that the antivirus definitions and antimalware software on the endpoint device are current and that the endpoint device firewall is active and current as well. Configure the firewall to prompt and confirm programs of unknown origin before allowing them to execute.

You can configure settings such as these using Group Policy. The security of the endpoint devices can be your first line of defense in mitigating a good number of security issues. Other solutions for endpoints can occur at the firewall. After an endpoint is authenticated, it can be scanned. If it violates corporate policy (which can be comprised of updated antivirus and antimalware software), that endpoint can be placed into a holding or staging area inside the DMZ for antivirus, antimalware, or policy updates before users are allowed to access to their Horizon View desktops.

You can also disable unneeded services on the endpoint operating system. Performing this action closes points of vulnerability for the operating system and reduces the attack surface that hackers can, and typically do, exploit.

View Agent

When securing the View Agent, use the policy settings in the View Agent Configuration Template. You can load this policy file in the Group Policy editor and apply various policies to enable and prevent specific functions of the View Agent. Some of the functions that can be applied to the View Agent are:

- **AllowDirectRDP** - Controls whether non-View clients can connect directly to Horizon View virtual desktops using the Microsoft Remote Desktop Protocol. When disabled, the View Agent permits only View-managed desktop connections through the View Client. The setting is enabled by default. Disable it to allow only View-controlled connections.
• **AllowSingleSignon** – Determines whether single sign-on (SSO) is used to connect Horizon View users to their virtual desktops. When SSO is disabled, users must re-authenticate after making a remote connection. This setting is enabled by default. Disable it to force users to enter their credentials a second time before being allowed to access their desktops: once for the remote connection, and again to access the Horizon View desktop.

• **CommandsToRunOnConnect** – Specifies the commands or scripts that are run when a Horizon View session is connected for the first time.

• **CommandsToRunOnReconnect** – Specifies the commands or scripts that are run when a Horizon View session is reconnected after a disconnection.

**Horizon View Desktops**

Many of the same principles that apply to View Client laptops and desktops also apply when you deploy Horizon View desktops. The objective is to minimize the attack surface while providing the best possible end-user experience.

• Disable unnecessary services and uninstall unneeded system and user components from the master image.

• Consider using Group Policy to maintain consistency across virtual desktops and verify that users cannot make modifications that might open the desktop to security vulnerabilities.

• Use the View Agent ADM templates to control the flow of information to and from the desktop. For example, disabling the clipboard prevents users from cutting and pasting information that might be confidential or otherwise potentially damaging to an organization’s security or intellectual property.

• Define an acceptable policy for recomposing or refreshing Horizon View desktops on a regular schedule to account for security patches, application patches and updates, and operating system updates. If you are deploying linked clones, refresh the master image.

**SSL Certificates**

Horizon View installs self-signed Secure Socket Layer (SSL) certificates when the product is installed.

**Note:** The default certificate installed when you install Horizon View is not signed by a Certificate Authority (CA).

Continuing to use these self-signed certificates can allow hackers and other unauthorized persons to perform man-in-the-middle (MITM) attacks. It is imperative to replace these certificates with trusted SSL certificates signed by a trusted Enterprise or commercial CA, such as a VeriSign or other certificate authority, before placing your Horizon View deployment into production.

All Horizon View clients, Security Servers, Composer Servers, and Connection Servers require valid SSL certificates. Before adding VMware vCenter™ and View Composer to the View Manager environment, verify that vCenter and View Composer have trusted certificates that are signed by a CA. If you install View Composer on the vCenter Server™, both components can use the same certificate, but it must be configured for each individual component.

Verify that all of the following Horizon View servers and components have valid SSL certificates:

• vCenter Server or vCenter Server Appliance

• View Connection Server

• View Composer Server

• View Security Server (when deployed)

• PCoIP Gateway

• Blast Secure Gateway

• View Transfer Server

• SAML 2.0 Authenticator
Figure 2 shows a typical SSL certificate that has been issued by a trusted Certificate Authority.

![Certificate](image)

Figure 2: SSL Certificate Issued by a Trusted Certificate Authority

To restrict the ability of hackers to intercept and obtain data, verify that your Horizon View deployment is properly protected by certificates issued by a trusted Certificate Authority. If a certificate is signed by a CA, it is embedded in the browser or located in a trusted database that the View Client accesses. When the View Client accepts the certificate, a secret key is sent, encrypted with the public key contained in the certificate. The secret key is then used to encrypt the traffic between the View Client and the server. For additional information on the use of SSL in your deployment, see VMware Horizon View Installation and Obtaining SSL Certificates for VMware Horizon View Servers.

**Load Balancing Configuration**

When configuring load balancers:

- Verify that they are configured to provide availability in the event of a load balancer failure. Typical deployments utilize load balancing clusters to continue operating if a single load balancer fails.

- Restrict administrative access to the load balancer configuration and operational functions to trusted staff members.

- Audit the load balancer configuration on a regular basis to verify that there has been no unauthorized access.

- Back up and store the configuration separately from the load balancers themselves to facilitate recovery.

If you are servicing large numbers of remote users, consider enabling SSL termination on the load balancer array to offload secure traffic from the View Security Servers. With SSL termination enabled on the load balancing array, SSL traffic can be balanced by multiple load balancer arrays. This can amount to a signature
performance increase when used with high-volume SSL traffic. Also, inbound traffic is decrypted at the load balancer array and passed on to the View Security Server for processing. This eliminates the need for decrypting the inbound SSL traffic at the View Security Servers and can reduce the processing load on them.

When you use SSL termination on load balancers, the nodes or hosts must reside in the same datacenter, to prevent unencrypted traffic from being sent over the Internet or any other untrusted zone.

**Note:** Use the external URL of the View Security Server, not the load balancer URL, to create the SSL certificate (See the VMware Knowledge Base article, View Administration Dashboard displays the View Connection Server in red and reports the error: The service certificate does not match the url.)

### Antivirus and Antimalware

Deploy a good antivirus and antimalware suite to protect Horizon View desktops against external attacks, and keep virus definitions up to date. Consider using VMware vCloud Networking and Security™ and VMware vShield Endpoint™ security for the Horizon View deployment, and use an integrated antivirus and antimalware suite to protect virtual desktops and minimize performance degradation when scanning many Horizon View desktops at the same time. If you install antivirus and antimalware on each Horizon View desktop, then stagger scanning of the desktops. Consider performing scans after hours to mitigate antivirus scanning storms, which increase I/O.

It is equally important that security software such as antivirus and antimalware be properly configured to notify the appropriate security personnel in the event of breaches and security software tampering.

Deploying vShield Endpoint security is the preferred and most efficient means for protecting virtual desktops from malware.

vShield Endpoint security integrates with products from the following vendors:
- Trend Micro
- McAfee
- Symantec
- Sophos
- Kapersky

### Integrating Horizon View into Active Directory

The Horizon View Connection and Horizon View Composer Servers are joined to an Active Directory domain. These servers are subject to all policies configured for the AD forest and domain unless explicitly blocked for those servers.

You can use Group Policy to further secure these servers. The View Group Policy Administrative Templates can help to lock down additional settings pertaining to the Horizon View deployment.

Before you configure and grant remote access to the Horizon View environment, care should be taken to ensure that the Windows operating system is fully updated with the latest operating system and security patches and that the antivirus and antimalware software is installed and fully updated. Performing these tasks reduces the attack surface while helping to mitigate unauthorized use or attacks on the View Connection and View Composer Servers.

Use Active Directory groups, Organizational Units, and Group Policy to restrict users to their entitled desktops. When more than basic security is required, employ two-factor authentication to enhance security and to protect end users against unauthorized access to their Horizon View desktops.
The Windows Security Wizard can be used to completely lock down the server operating system to prevent unauthorized access to the server.

**Caution:** Care should be exercised when choosing to apply Windows Security Wizard recommendations, which can lead to lockdown of the server and render it useless. Apply only those policies appropriate to your organization’s security.

Ensure that all required applications on the View Connection and Composer Servers are properly configured and running before you initiate a Windows Security Wizard scan on the server to prevent any required View Connection and View Composer Server application component lockouts. As with the View Security Server, you can configure security protocols and cipher suites that are compatible with the View Connection Server. You can also define a global acceptance policy that can apply either to all View Connection Servers in a replicated group or to individual View Connection Servers.

The default policies and the procedures for configuring them have been updated for VMware Horizon View 5.2. For more information on configuring policies and ciphers for earlier versions of View, see the VMware Knowledge Base article, *Configuring cipher suites and security protocols on a View Connection Server instance or Security Server in View 4.5 and later*.

The View ADM and Agent templates can also provide extra levels of security beyond the basic configuration of the VMware Horizon View product. The ADM template file provides security settings for the View Agent that apply only to computer configuration settings. Security settings for the View Client are stored on the host machine in the Registry under the following key: `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Security`.

For more information on the Horizon View security template files, see *VMware Horizon View Security*.

---

**External Deployment**

When you configure the Horizon View deployment to allow remote access, the following tasks are completed:

- Move the load balancers configured for the internal deployment to the DMZ, between the internal and external firewalls, and reconfigure their network properties to allow them to function there. (Omit this task if the load balancer or load balancing array is already deployed in the DMZ.)

- Install the View Security Servers, and pair them with their respective View Connection Server instances.

- Deploy the View Security Server(s) in the DMZ to provide enhanced authentication for remote users connecting to their entitled Horizon View desktops.

- Install or update trusted Certificate Authority–signed SSL certificates on the View Security Server(s) and the load balancing array to match the external URL of the View Security Server(s).

- If required, configure enhanced two-factor authentication security, such as RADIUS or RSA SecurID, and other supported two-factor solutions for remote access to entitled Horizon View desktops. For more information on two-factor configuration, see the References section of this document.

- Configure View Clients to access internal View Security Servers using trusted CA-signed certificates. As of Horizon View 5.2, Horizon View users can replace self-signed certificates with trusted CA SSL certificates to access their entitled Horizon View virtual desktops.

For more information on remote Horizon View deployments, see *VMware Horizon View Architecture Planning* and *VMware Horizon View Security*.
Figure 3 illustrates a Horizon View deployment that has been configured to allow remote access. The load balancing array and the security servers are deployed in the DMZ, with the View Security Servers each paired to an instance of View Connection Server in the internal or trusted network.

Security Server Considerations

The View Security Server provides remote access for users connecting to the Horizon View environment without connecting to the internal corporate network. It forces all untrusted or Internet traffic through its secure PCoIP gateway or SSL tunneled connections for Microsoft Remote Desktop Protocol (RDP). The View Security Server enforces strong authentication before allowing users who connect remotely to access their entitled Horizon View desktops.

- When securing the View Security Server, care should be taken to ensure that the Windows operating system is fully updated with the latest operating system and security patches.

- Verify that antivirus and antimalware software is installed, fully updated, and functioning properly. The objective is to reduce the attack surface of the server so that any risks to the View Security Server can be mitigated. This is especially true if you are terminating SSL traffic at the load balancer array, because traffic is not secure after it leaves the View Security Server. It is important that all patches and security software such as antivirus and antimalware software be fully updated, configured, and functioning properly.
Consider running the Windows Security Wizard to completely lock down the server operating system to allow only authorized access to the server.

The Windows Security Configuration Wizard can perform the following tasks for you:

- Disable any unnecessary services and close firewall ports.
- Create stronger security policies than those created using security templates.
- Create security policy that can be deployed using Group Policy.

**Caution:** Care should be exercised when choosing to apply Windows Security Wizard recommendations, which can lead to lockdown of the server and render it useless. Apply only those policies appropriate to your organization’s security.

When using the Windows Security Wizard, ensure that the required applications are configured and running on the server at the time of configuration.

If you are terminating SSL at the load balancer or array in the deployment, use the same certificates on the load balancer as you use on the View Security Server to prevent traffic from being blocked because of an untrusted certificate. See the VMware Knowledge Base article, View Administration Dashboard displays the View Connection Server in red and reports the error: The service certificate does not match the url. SSL termination is described in SSL Certificates and Load Balancing Configuration.

Horizon View provides additional methods for securing the server by restricting traffic to specific firewall ports. You must properly configure the primary and secondary firewalls that make up the DMZ to allow Horizon View desktops and the View Connection Server(s) to communicate with one another. Refer to your firewall or software vendor’s documentation for information on configuring specific firewalls.

For additional information on firewall port configuration for the View Security Server, see VMware Horizon View Architecture Planning. For more information about the services and ports required on the View Security Server, see VMware Horizon View Security.

**Firewall and DMZ Configuration**

For any organization, the firewall plays a crucial role in the security for the entire organization. It is the first obstacle that hackers must get through before they gain unauthorized access to corporate data. It is crucially important that the firewall be protected by closing all unnecessary ports and opening only ports that are absolutely necessary for the daily operations of the organization.

Conduct periodic port scans on the primary and secondary firewalls to ensure the firewall policy is correctly implemented and does not allow unauthorized access into the DMZ, and furthermore, into the trusted zone or Intranet. The DMZ is defined as the space between the primary firewall and secondary firewalls, and is the second line of defense in the case of a security breach of the primary firewall.

Back up the firewall configuration before and after any rule change, addition, or deletion.

Restrict access to the administrative functions of the firewall, and audit them periodically to ensure that only authorized personnel gain access to the firewall.

Conduct traffic pattern analysis on what traffic is allowed inside the primary firewall, into the DMZ, and past the secondary-level firewall that protects the corporate intranet. Use stateful inspection-type firewalls capable of analyzing the attributes of the connections, and the status of the connections, made to the firewall.

Inside of the DMZ, when configuring the port traffic and rules for allowing access to Horizon View—as well as to other applications running in the organization—consider the possibility of restricting application traffic to the specific hosts that the traffic is intended for by specifying hostname or IP addressing for the hosts in the rule set.
For example, you can establish a rule that allows Horizon View SSL traffic inside the firewall only to the load balancers, which then directs the traffic to the View Security Servers, and so forth, until an authenticated connection is established with an entitled Horizon View desktop.

Conduct a careful and thorough analysis of the traffic traversing your firewall to ensure that necessary traffic to conduct the business operations is not impacted.

Two-Factor Authentication

When using two-factor authentication to provide remote access to the Horizon View deployment, consider the following options.

SecurID

When enhanced security for remote access to Horizon View desktops is required, deploy two-factor authentication (2FA) to provide enhanced authentication to Horizon View Clients. Two-factor authentication can greatly enhance the security of your Horizon View desktops by ensuring that all Horizon View Clients go through a stringent authentication process before being allowed to access their entitled desktops.

Two-factor authentication requires two forms of authentication for access to Horizon View desktops, data, and other protected information. It usually consists of something you have or posses, such as smart cards, common access cards (CAC), hardware-based or software-based tokens, and something you know, such as a personal identification number (PIN) or other code. In two-factor authentication, the user enters a code or inserts a smart card and enters their PIN. If authenticated, users can access their entitled Horizon View desktops.

When using a properly configured two-factor authentication for Horizon View, you can be assured that all access to the Horizon View environment is secure, and that only authorized users can access their entitled Horizon View desktops.

Note: When 2FA is enabled on the View Connection Server, users must use 2FA to gain access to their entitled Horizon View desktops.

Horizon View is compatible with many two-factor authentication solutions from vendors such as RSA SecurID, VASCO DIGIPASS, SMS Passcode, and SafeNet. These vendors provide an integrated two-factor authentication solution for VMware Horizon View. More information on the deployment and configuration of their two-factor solutions for Horizon View is available on the vendors’ Web sites.
RADIUS
As of VMware View™ 5.1, Remote Access Dial-in User Server (RADIUS) is supported for two-factor authentication. You can configure the View Connection server so that users are required to use RADIUS for authentication. If you deploy multiple View Connection servers—for instance, one for remote access and one for local access—each of the servers can use different authentication methods. In this case, users who access their Horizon View desktops over the Internet would need to use two-factor authentication, while users already connected to the corporate intranet could be authenticated using Active Directory. Figure 4 depicts a typical RADIUS configuration.

![High-Availability RADIUS Configuration with a Single View Connection Server](image)

When deploying RADIUS, consider deploying the RADIUS servers in a high-availability configuration, using primary and secondary servers to mitigate the likelihood of user authentication outages due to server failure. The most basic Horizon View setup with RADIUS authentication consists of a single View Connection Server and a single RADIUS Server. All other servers deployed are optional.
Security vendors who support View 5.1 and later include:

- ActivIdentity
- Nordic Edge
- PhoneFactor
- SafeNet
- Symantec
- Signify

If you deploy externally facing View Connection Servers without View Security Servers, deploy RADIUS with Horizon View to force users to enter their username and a passcode at the View Client login.

For example, if you enable challenge and response, users accessing their Horizon View desktops enter their login credentials into the View Client login, at which time a Short Message Service (SMS) text message or email message with a PIN is sent to their smart phone. The users then enter the PIN into the View Client to access their Horizon View desktops.

This example could be a viable solution when externally facing View Connection Servers are deployed.

**PCoIP**

For remote connectivity, proper configuration of a secure access protocol, such as PCoIP, is essential. PCoIP uses the User Datagram Protocol (UDP) instead of the Transmission Control Protocol (TCP) to encapsulate video packets more efficiently than RDP. This secure protocol works exceptionally well over WAN and 3G technologies.

The PCoIP secure gateway is installed on the View Security Server. It uses AES-128-bit encryption and supports enhanced session control for Horizon View. This encryption can be changed to stronger encryption if required. To function properly with PCoIP, the Security Server requires inbound and outbound UDP port 4172 and TCP port 4172 to be opened. The View Connection Server sends the destination IP and port numbers for PCoIP to the View Client. It uses addresses and port numbers that belong to the View Security Server, not the Horizon View desktop, to route all PCoIP traffic through the View Security Server.

The View Client initiates a connection from the Internet to the load balancer in the DMZ, which passes the connection to the View Security Server. At this point, the View Security Server can initiate a PCoIP connection to the Horizon View desktop on behalf of the View Client without actually traversing the corporate network. See the VMware Knowledge Base article, Configuring PCoIP Secure Gateway in VMware Horizon View, for further details.

**Using vCloud Networking and Security to Secure the Horizon View Environment**

VMware vCloud Networking and Security provides tools to virtualize and secure your Horizon View deployment and protect it from network-based attacks. VMware vShield App™ helps you deploy a distributed, per-port firewall with the ability to create firewalls on a per-virtual Network Interface Card (NIC) basis. This enables you to control what traffic a Horizon View desktop can receive and where it can receive it from, as well as where it can send traffic.

VMware vShield App provides unified, central control of firewalls, and vCloud Networking and Security also includes data security integration with RSA security Data Loss Prevention (DLP) APIs. With vShield App, you can create Horizon View desktop zones—for instance to isolate contractors, high-risk Web browsing desktops, and offshore contractor desktops—and place them in their own security zones. With this configuration, you can allow them to communicate or totally block communication outside of their security zone. You can further configure security zones for multi-tiered applications, servers, and systems that require compliance. Using security zones can enable antivirus scanning offload, which, if processed on each individual virtual desktop, can lead to scanning storms and increased I/O demands on the virtual desktop infrastructure, as mentioned in Antivirus and Antimalware.
Sample Automobile Manufacturer Use Case Scenario

The following use case scenario illustrates the use of vCloud Networking and Security to secure a Horizon View desktop infrastructure as well as other applications and infrastructure running in a virtual datacenter. It takes into account the following requirements and considerations:

• Different sets of users require access to different sets of resources.
• Horizon View desktops are deployed to three sets of resource pools:
  - Line Manager desktops, which belong to a Line Managers Active Directory group
  - Line Service desktops, which belong to a Service Technicians Active Directory group
  - Browsing desktops with both Line Managers and Service Technicians Active Directory group entitlements
• vCloud Networking and Security virtual firewall rule configuration:
  - Line Managers need access to Build Manifest Servers.
  - Line Service Technicians need access to Line Control Servers.
  - Both need access to the Internet.
  - All other access must be restricted.

Figure 5 illustrates a solution to the use case scenario without the use of VLANs.
Monitoring the Horizon View Environment

Monitor your Horizon View deployment periodically for security and performance issues. Consider deploying intrusion detection and antivirus and antimalware software to notify appropriate personnel when attacks are imminent, if you have not already done so.

Monitor the firewall for unused open ports that a hacker might exploit. If you use software firewalls—which are strongly recommended—verify that the software is updated and patched in a timely manner to prevent security exploits, including those identified by your firewall vendor.

In addition to monitoring the deployment for security, you should constantly monitor your Horizon View deployment to verify that the end-user experience is maintained when users access their entitled Horizon View desktops remotely.

One solution for monitoring the Horizon View deployment for performance is VMware vCenter Operations Manager for View™. In addition to monitoring Horizon View, it enables monitoring of the vSphere compute, memory, storage, and network infrastructure that hosts Horizon View.

vCenter Operations Manager for View gives you a complete performance picture of the Horizon View deployment and allows you to tailor collection metrics and define minimum and maximum thresholds for alerts.

For more information on vCenter Operations Manager for View, see the VMware vCenter Operations Manager for Horizon View documentation.

Conclusion

Threats to security continue to evolve, so no guide to this topic can ever be considered complete. Nevertheless, this paper covers the most important security considerations for Horizon View deployments, including examples of internal and external deployments.

There are many options for providing security for a Horizon View deployment while maintaining a high-quality end-user experience. When planning security for your environment, review all applicable corporate policies and requirements, and consider each security option carefully. Remember, the objective is to keep the corporate intellectual property and resources safe and secure while providing an end-user experience that does not inhibit productivity.
References

vSphere Security: ESXi 5.1, vCenter Server 5.1
VMware Horizon View Architecture Planning
VMware Horizon View Security
Obtaining SSL Certificates for VMware Horizon View Servers
Horizon View 5 with PCoIP Network Optimization Guide
Horizon View Persona Management Deployment Guide
Mark Benson’s RADIUS Configuration Blog
Using Two-Factor Authentication with VMware Horizon View
Configuring cipher suites and security protocols on a View Connection Server instance or Security Server in View 4.5 and later (1021466) – VMware Knowledge Base article
View Administration Dashboard displays the View Connection Server in red and reports the error: The service certificate does not match the URL (2021432) – VMware Knowledge Base article
View 5.1 Security Servers and SSL – VMware Horizon View Community discussion
View Administration dashboard reports the error: Server’s certificate cannot be checked (2000063) – VMware Knowledge Base article
Configuring PCoIP Secure Gateway in VMware Horizon View (1036208) – VMware Knowledge Base article
vSphere Security Hardening Guide
Secure Remote Access with View and PCoIP – Office of the CTO blog post
VMware Integrated Partner Solutions for Networking and Security
VMware vCenter Operations Manager for Horizon View

About the Author

Charles A. Windom Sr. is a Senior Technical Marketing Manager at VMware. In this role, his primary focus is to develop technical content to aid in evaluation and implementations of VMware Horizon View and VMware ThinApp®. Charles’s background includes roles as a Solutions Architect in the VMware Microsoft Solutions organization. His previous positions include Solutions Architect with Digital Equipment, Compaq, Hewlett Packard, Hitachi Data Systems, Brocade Communication, Siebel Systems, and LSI Logic Corporation.

The author would like to thank Mark Benson, Rob Randell, and Ravi Kumar for their contributions to this paper.