VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution

Introduction

Customers today are looking to desktop virtualization to deliver desktop services to end-users across a variety of locations. These end-users not only reside on the Local Area Network (LAN) but there is an increasing demand for end-users across the Wide Area Network (WAN) to access desktops hosted in corporate datacenters.

As with other remote access technologies, PCoIP display protocol performance depends on the VPN performance, available network bandwidth and network latency. The WAN requirement can pose a challenge to IT organizations that not only need to deliver desktop services to these end-users but must also do so in a secure manner. For this requirement many customers have turned to SSL VPN solutions to provide secure connections to end users accessing virtual desktops from branch and home office as well as other remote locations.

VMware View

VMware® View™ delivers a desktop solution enabling end-users to access virtual desktops running in the corporate datacenter from a variety of devices and locations. Using VMware View with the PC-over-IP (PCoIP) display protocol, end-users benefit from a rich desktop experience on the LAN as well as across the WAN.

VMware is proud to work with partners like Cisco Systems who deliver solutions to enable secure connections to end-users based on SSL VPN technologies. With solutions such as the Cisco Adaptive Security Appliances (ASA) with the Cisco AnyConnect Secure Mobility client, an end-user is able to connect with PCoIP from a remote location across an encrypted connection back to the datacenter where their desktop resides.

Cisco Adaptive Security Appliances (ASA)

The Cisco® ASA 5500 Series Adaptive Security Appliance is a purpose-built platform that combines best-in-class security and VPN services for small and medium-sized business (SMB) as well as enterprise customers. The Cisco ASA 5500 Series enables customization for specific deployment environments and options, with special product editions for secure remote access (SSL/IPsec VPN), firewall, content security, and intrusion prevention.

The Cisco Secure Remote Access solution offers flexible VPN technologies for any connectivity scenario, with scalability up to 10,000 concurrent users per device. It provides easy-to-manage, full-tunnel network access through SSL, Datagram Transport Layer Security (DTLS), IPsec VPN client technologies, Cisco AnyConnect Secure Mobility optimized for the Cisco IronPort® Web Security Appliance, advanced clientless SSL VPN capabilities, and network-aware site-to-site VPN connectivity, enabling secure connections across public networks to remote end-users including those connecting to VMware View virtual desktops using the PCoIP display protocol.

Benefits of a Cisco Secure Remote Access solution include:

- **SSL and DTLS based full network access** – Provides network-layer remote-user connectivity to virtually any application or network resource including VMware View virtual desktops using the PCoIP display protocol. The Cisco AnyConnect Secure Mobility client will automatically adapt its tunneling protocol to the most efficient method based on network constraints, and is the first VPN product to use the DTLS protocol to provide an optimized connection for latency-sensitive traffic, such as voice-over-IP (VoIP) traffic or TCP-based application access. By supporting SSL, DTLS, and IPsec-based remote-access VPN technologies, the Cisco ASA 5500 Series delivers unsurpassed flexibility to meet the needs of the most diverse deployment scenarios.
- **Superior clientless network access** - Provides access to network applications and resources, regardless of location, without the need for desktop VPN client software. Using the ubiquity of SSL encryption the Cisco ASA 5500 Series delivers clientless access to a variety of applications and services such as VMware View using the RDP display protocol today and anticipated future support for PCoIP.
- **Scalability and resiliency** - Support for up to 10,000 simultaneous user sessions per device, with the ability to scale to tens of thousands of simultaneous user sessions through integrated clustering and load-balancing capabilities. Stateful failover features deliver high-availability services for unsurpassed uptime.

Accessing a VMware View Desktop With Cisco ASA

The Cisco ASA SSL VPN remote access solution supports two methods for remote VMware View clients to securely connect to virtual desktops in the datacenter.

Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility client provides remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

AnyConnect runs on Microsoft Windows, Mac OS X, Linux, and Windows Mobile and supports connections to IPv6 resources over an IPv4 network tunnel. Administrators can configure the AnyConnect client to auto-launch a pre-installed VMware View client on the user desktop.

Datagram Transport Layer Security (DTLS) avoids latency and bandwidth problems associated with regular SSL connections and is a standards-based SSL protocol that provides a low-latency data path using UDP.

DTLS enhances the performance of real-time applications such as the VMware View Client with PCoIP, a UDP display protocol.

Clientless SSL VPN

Utilizing the Smart Tunnel technology through a web browser enables VMware View virtual desktop access without the need to provide a full tunnel connection to the end-point device using AnyConnect. Utilizing AnyConnect will provide the maximum end-user experience since PCoIP can be used for the display protocol.

With the Smart Tunnel technology, a secure connection is established between a TCP-based application (web browser) and the Cisco ASA at the private site. This “Smart Tunnel” technology enables access to VMware View client when Microsoft RDP display protocol is selected.

Solution Topology and Connection Flow

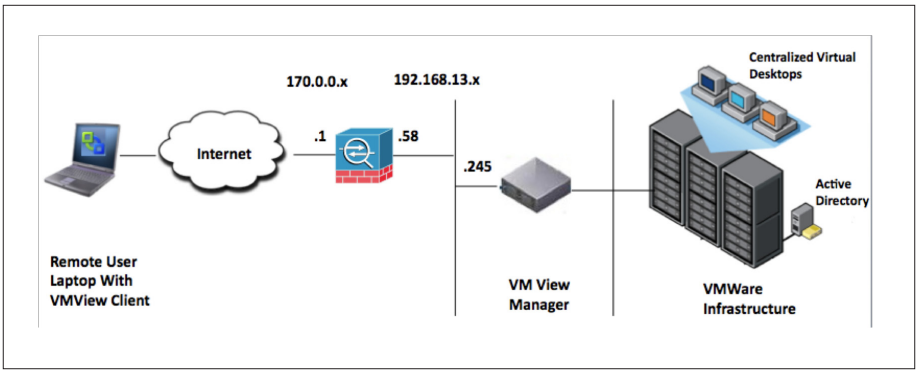

Figure 1. Topology

Connection Flow

1. The remote end-user establishes an SSL VPN connection with the ASA VPN Gateway using either the AnyConnect Client or a Smart Tunnel.
2. The end-user then uses the VMware View Client to communicate across the secure tunnel and authenticate with the VMware View Manager in the corporate datacenter.
3. After successful authentication the VMware View Manager displays the available virtual desktops available to the end-user.
4. The end-user then selects and connects to the desired VMware View desktop to establish the virtual desktop session.

Summary

VMware View and the Cisco ASA together create a solution for remote end-users to securely access virtual desktops residing in corporate datacenters. With support for DTLS, the Cisco ASA delivers a solution for securely transporting UDP based network traffic such as the PCoIP display protocol to connect remote end users with their corporate virtual desktop. With the AnyConnect Secure Mobility client and clientless Smart Tunnel technology, end-users have choices to securely connect to their virtual desktop in the datacenter.

References and Additional Resources

VMware

VMware View Website
http://www.vmware.com/products/view/

VMware View Manager Datasheet
http://www.vmware.com/files/pdf/VMware-View-Manager-4-DS-EN.pdf

VMware View Documentation
http://www.vmware.com/support/pubs/view_pubs.html

Cisco

Cisco ASA Website
http://www.cisco.com/go/asa

Cisco ASA Datasheet
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

Cisco ASA Documentation
http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

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