



P r o f e s s i o n a l E x p e r t i s e D i s t i l l e d

Citrix Access Gateway VPX 5.04 Essentials

A practical step-by-step guide to provide secure remote access
using the Citrix Access Gateway VPX

Andrew Mallett

[PACKT] enterprise 
PUBLISHING professional expertise distilled

Citrix Access Gateway VPX 5.04 Essentials

A practical step-by-step guide to provide secure remote access using the Citrix Access Gateway VPX

Andrew Mallett



BIRMINGHAM - MUMBAI

Citrix Access Gateway VPX 5.04 Essentials

Copyright © 2013 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: January 2013

Production Reference: 1170113

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-84968-822-2

www.packtpub.com

Cover Image by Artie Ng (artherng@yahoo.com.au)

Credits

Author

Andrew Mallett

Project Coordinator

Abhishek Kori

Reviewers

Jack Cobben

Daniele Tosatto

Proofreader

Lydia May Morris

Acquisition Editor

Rukhsana Khambatta

Indexers

Hemangini Bari

Tejal Soni

Lead Technical Editor

Ankita Shashi

Graphics

Aditi Gajjar

Technical Editor

Kaustubh S. Mayekar

Production Coordinator

Arvindkumar Gupta

Copy Editors

Brandt D'Mello

Laxmi Subramanian

Aditya Nair

Alfida Paiva

Ruta Waghmare

Cover Work

Arvindkumar Gupta

About the Author

Andrew Mallett has worked in the IT industry for more years than he cares to mention — well, since 1986 — and with Citrix technologies since Metaframe 1.8 in 1999. He not only has Citrix skills and certification, but also teaches Linux, Novell, and Microsoft's official courses and supports many of these products. Being well-versed and certified in Linux gives him interest and skills in security and remote access, which made this an ideal book for him to write, combining Linux and Citrix into one product and book.

He currently freelances as an instructor and consultant in the UK. You can follow him on twitter, @theurbanpenguin, or visit his website, <http://www.theurbanpenguin.com>.

This is my first book; having authored courseware before, venturing into books made this the next logical step. I particularly wish to thank Maddie, my first granddaughter; having my first grandchild and book in the last one year is amazing, and moreover, Maddie gave me the happiness and purpose to see it through.

About the Reviewers

Jack Cobben, with over thirteen years of systems management experience, is no stranger to the challenges enterprises can experience when managing large deployments of Windows systems and Citrix implementations. Jack writes in his off time for his own blog, www.jackcobben.nl, and is active on the Citrix support forums. He loves to test new software and shares the knowledge in any way he can. You can follow him on twitter, via @jackcobben.

While he works for Citrix, Citrix didn't help with, or support, this book in any way or form.

Daniele Tosatto is a Senior Systems Engineer based in Venice, Italy. He is a Microsoft Certified IT Professional, Microsoft Certified Technology Specialist, Microsoft Certified Solutions Expert, and Citrix Certified Administrator and has been working with Microsoft products since 2000 as a system administrator. In February 2008, he started working for the first Italian Citrix Platinum Partner. He is focused on Active Directory design and implementation, application virtualization and delivery, and IT infrastructure management.

He maintains a blog at <http://www.danieletosatto.com>, and he is the author of the book *Citrix XenServer 6.0 Administration Essential Guide*, Packt Publishing.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<http://PacktLib.PacktPub.com>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Instant Updates on New Packt Books

Get notified! Find out when new books are published by following [@PacktEnterprise](#) on Twitter, or the *Packt Enterprise* Facebook page.

Table of Contents

Preface	1
Chapter 1: Getting Started with the Citrix Access Gateway Product Family	7
Security and Remote Access Solutions addressed by Citrix Access Gateway	8
Citrix Access Gateway hardware	10
NetScaler Model 2010 Appliance	10
NetScaler Model MPX 5500 Appliance	11
Citrix Access Gateway versions	12
Access Gateway Milestones	12
Access Gateway 10	13
Access Gateway 9.3 Enterprise Edition	14
Access Gateway 9.2 Enterprise Edition	14
Access Gateway 5.x	15
Citrix Access Gateway VPX Edition	15
Designing a secure Remote Access solution	17
Availability	17
Using ICA Proxy to access XenApp/XenDesktop	18
Ensuring there is no path for a single protocol to traverse the DMZ	18
Resolving remote access issues using Citrix Access Gateway	19
If you need access to other resources, we have full VPN connections	20
Authentication	20
PKI Certificates	20
Summary	20
Chapter 2: Licensing the Citrix Access Gateway	21
Overview of licensing CAG	21
License Grace Period	22
Platform License	22
Universal License	23

Concurrent connections	23
Citrix Access Gateway Express	23
License Server options	24
Obtaining licenses	25
Deploying Microsoft Windows Server and VPX License Server	25
Installing License Server 11.10	26
Importing License Server VPX into Citrix XenServer	28
Importing licenses and management	30
License Server Administration	33
Securing the dashboard	34
Securing License Server with HTTPS	35
Summary	36
Chapter 3: The Citrix Access Gateway Initial Setup	37
Understanding the network architecture	37
Downloading the virtual appliance from Citrix	38
Importing the Citrix Access Gateway into VMware	39
Importing the Citrix Access Gateway into XenServer	39
Initiating the Access Gateway setup from the command line	40
Completing the initial configuration from the web portal	44
Setting the admin password	45
Add a static route to a private network	45
Licensing the Citrix Access Gateway	47
Adding SSL certificates	48
Monitoring the Citrix Access Gateway	52
Summary	54
Chapter 4: Configuring a Basic Logon Point for XenApp/XenDesktop	55
Identifying the need for using CAG as a remote access solution	56
Configuring a Citrix Web Interface site for use with the Citrix Access Gateway	57
Web Interface placement	58
Configuring a website for remote users	59
Changing the Secure Access method	62
Configuring an Access Gateway basic logon point	65
Logon point	66
XenApp and or XenDesktop access controls	70
Secure Ticket Authority	71
Accessing XenApp Server farms securely with the Citrix Access Gateway	72

Extending the basic logon point to access other internal web-based resources	73
Keeping your users happy	77
Auditing access to the Citrix Access Gateway	78
Summary	80
Chapter 5: Creating Authentication Profiles	81
Authentication profiles	82
Creating a RADIUS authentication profile	83
Configuring Gemalto Protiva	86
Configuring SafeWord	87
Creating RSA SecurID authentication profiles	88
Creating LDAP authentication profiles in Microsoft's Active Directory	90
Authentication using the Active Directory sAMAccountName	92
Authenticating using the Active Directory userPrincipalName	93
Tracking user access	94
Creating LDAP authentication profiles in Novell's eDirectory Directory	94
Creating LDAP authentication profiles to Linux openLDAP	95
Customizing the Citrix Access Gateway logon page	96
Allowing users to change passwords on the logon page	98
Implementing two-factor authentication on the Citrix Access Gateway	100
Summary	102
Chapter 6: Beyond the Basics	103
Adding universal licenses	103
Citrix Access Gateway plug-in installation	104
Obtaining the plug-in	105
Installing the plug-in	105
Configuring the plug-in properties	107
Integrating the Access Gateway plug-in with the Citrix Receiver	111
Distributing the Access Gateway plug-in with the Citrix Merchandising Server	112
Configuring deliveries with the Merchandising Server	114
Summary	117
Chapter 7: Address Pools	119
Creating address pools	119
Before we connect with the plug-in	122
Ping after the VPN is created with the plug-in	123

Accessing the welcome page on the web server	123
Smart logon points use universal licenses	125
System Administration Options	126
Networking	127
Appliance failover	127
Name service providers	127
Static routes	128
Address pools	128
Deployment mode	128
Password	128
Date and time	129
Licensing	129
Logging	129
Summary	130
Chapter 8: Device Profiles and Endpoint Analysis	131
Device profiles	132
File	133
Process	133
Registry	134
Operating System	135
Ports	136
Building an effective scan expression	137
Installing the endpoint analysis plug-in	138
Control Access to network using device profiles	141
Summary	141
Chapter 9: Defining Network Resources	143
Network resources	143
Network lists	148
General Properties	149
Protocols and port ranges	149
Introducing the Citrix Branch Repeater	150
Citrix Branch Repeater products	150
Summary	153

Chapter 10: SmartAccess Logon Points	155
Defining SmartAccess logon points	155
General Properties	157
Authentication	158
Defining the term Logon Point Visibility	160
Branding the logon point	161
Summary	162
Chapter 11: Linking It All Together with SmartGroups	163
Defining SmartGroups	164
General Information	164
Home Page	165
Group Criteria	166
Logon Points	166
Device Profiles	166
Group Membership	167
Group Settings	169
Network Resources	169
Address Pools	171
Advanced Properties	172
Defining SmartGroup priority	174
Summary	175
Chapter 12: Connecting to SmartAccess Logon Points	177
Delivering the Access Gateway plug-in	177
Configuring Access Gateway Plug-in settings	180
Managing the client plug-in	182
Connecting to resources on the private network	184
Summary	186
Chapter 13: Monitoring the Citrix Access Gateway	187
Accessing and interpreting logfiles	187
System Information	188
Running Information	189
Active Sessions	190
Configuration and Warnings	192
Audit Log	192
Info Log	193
EPA Log	193
Debug Log	193

Table of Contents

Logfile settings and log transfer	194
Creating configuration snapshots and importing firmware updates	196
Implementing appliance failover	198
Configuring the master device	199
Configuring the slave device	200
Summary	202
Chapter 14: Command Line Management of the Citrix Access Gateway	203
Enabling SSH access to the command line	203
Managing the Citrix Access Gateway from the command line	205
Express Setup	205
System	206
Troubleshooting	207
Help	209
Summary	210
Index	211

Preface

No matter how new you are to Citrix or for how long you have used it, we are going to show you how you can extend the use of Citrix products to beyond the confines of your corporate network, making full use of the "any device anywhere" tag line used in Citrix marketing. Citrix Access Gateway can provide full VPN access to your network or simple ICA Proxy, and Citrix Access Gateway VPX 5.04 Essentials will show you how to step through the complete process of configuring the appliance. Providing easy-to-follow guides that you will be able to follow as a seasoned Citrix professional or newbie, this book will take you through the full and complete deployment of the appliance.

What this book covers

Chapter 1, Getting Started with the Citrix Access Gateway Product Family, will describe the purpose of Citrix Access Gateway and the models that are available and their associated features. This chapter will serve as a good introduction to the product range and will help in choosing the correct model to meet a required business need.

Chapter 2, Licensing the Citrix Access Gateway, will walk you through Citrix licensing and its available options. You will discover the MyCitrix website, where licenses are obtained, and this will help with the assignment of hostnames to licenses. Licenses can be delivered from CAG or from a specific license server.

Chapter 3, The Citrix Access Gateway Initial Setup, will enable you to complete the first step in using CAG, which is to import it into our virtualization hosts and to configure networking, passwords, and adding SSL certificates.

Chapter 4, Configuring a Basic Logon Point for XenApp/XenDesktop, will provide guidance in the usage of the platform license, which you can use to establish unlimited connections to XenApp/XenDesktop servers and is widely used in this manner as an ICA Proxy. We will look at how to create this proof-of-concept system by creating a basic logon point and using authentication at the web interface server. This is the simplest form of CAG and provides a quick and easy start into using this system.

Chapter 5, Creating Authentication Profiles, will walk you through the authentication at the Citrix web interface, which is a simple solution but limits the usage of CAG; that is, being limited to just basic logon points. From a security perspective, passing authentication to the web interface server is allowing traffic to pass to another device that, as yet, had not been authenticated; authentication should be handled at the point of entry and nowhere else.

Chapter 6, Beyond the Basics, will introduce SmartAccess logon points and what is available with the universal licenses. Not only can we connect to XenApp and XenDesktop, but we now also have full VPN access to internal resources, such as internal e-mails, intranets, and network file shares.

Chapter 7, Address Pools, will show you how Address Pools allow your SmartAccess clients to be issued with an IP address to access internal resources. These may be required for some services that do not allow multiple connections from a single device.

Chapter 8, Device Profiles and Endpoint Analysis, will talk about using device profiles with SmartAccess, which enables us to identify different classifications of client machines the device profiles can control (which resources they can access and which policies will apply if they access XenApp or XenDesktop). Typically, we may need to be able to differentiate between corporate-managed computers and personal computers.

Chapter 9, Defining Network Resources, will walk you through CAG SmartAccess, which allows you access not only to Citrix XenApp and Citrix XenDesktop but also to internal resources, such as network file shares and e-mails. In this chapter, we will look at specifying network resources that we wish our users to have access to and those that they should not.

Chapter 10, SmartAccess Logon Points, will talk about how, when we are nearing the end of the configuration, we add SmartAccess logon points to the management console, providing full VPN access to internal networks.

Chapter 11, Linking It All Together with SmartGroups, will discuss Smart Groups that enable resources to be linked to logon points. These are added through the management console and can be described as the glue of the SmartAccess solutions.

Chapter 12, Connecting to SmartAccess Logon Points, will investigate how we can connect to our newly created SmartAccess logon points by using a web browser or the secure access plug-in.

Chapter 13, Monitoring the Citrix Access Gateway, will discuss how to monitor and maintain CAG. Having set up the gateway, it is important to be able to keep it running effectively. This will involve monitoring connections and logs, backing up the configuration with snapshots, and upgrading the firmware. Once we have this in the bag, we need to look into providing high availability using appliance failover.

Chapter 14, Command Line Management of the Citrix Access Gateway, will explain using the command line, and we will investigate some of the options available. Although most management is maintained via the web console, some elements can be managed from the command line, and we look at when and why we use this.

What you need for this book

To make full use of this book, you will need to have basic knowledge of Citrix products such as XenApp (or its predecessor, Presentation Server) or XenDesktop, and we will be implementing or investigating remote access solutions. Although no prior knowledge of virtual private networks is required, we would expect that you have basic grounding in IP-based networks and routing.

Who this book is for

This book is aimed at system administrators implementing or working with the Citrix Access Gateway 5.x virtual appliance, and it is also for those who are looking for a detailed handbook on the day-to-day administrative tasks that managing a Citrix remote access solution entails.

Conventions


In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.


Code words in text are shown as follows: "On 64-bit systems, this defaults to `c:\Program Files (x86)\Citrix`."

Any command-line input or output is written as follows:

```
xe vm-import -s 192.168.0.12 -u root -pw Password1  
filename="c:\tmp\cag_5.0.4.223500.xva
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "If using the CAG as License Server, the CAG name must be in the **HOST ID** field".

[ Warnings or important notes appear in a box like this.]

[ Tips and tricks appear like this.]

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book – what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to feedback@packtpub.com, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books – maybe a mistake in the text or the code – we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/support>, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from <http://www.packtpub.com/support>.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at questions@packtpub.com if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Getting Started with the Citrix Access Gateway Product Family

If you have ever tried navigating the range of products and vendor websites, you will be able to sympathize with those poor souls trying to come to terms with all of the different options that Citrix has for the Access Gateway products. So many choices! Soon, you will also find out that the costs of these products will vary from nothing to many thousands of dollars. The aim of this introduction is to help you become familiar with the range and make some informed decisions about which product is right for you. Throughout the book, we will work with the VPX edition (virtual appliance); however, most of the configuration remains consistent between the models. Additionally, at this stage, we also need to show you where **Citrix Access Gateway (CAG)** will fit into your corporate remote access and security environment.

Specifically, in this chapter, the following topics will be looked at in detail:

- Security and Remote Access solutions addressed by CAG
- Citrix Access Gateway hardware
- Citrix Access Gateway specifications
- Citrix Access Gateway versions
- Citrix Access Gateway VPX
- Designing a secure Remote Access solution

Security and Remote Access Solutions addressed by Citrix Access Gateway

Firstly, let us address a little of the history of Citrix Systems, the purpose of CAG, and why this is used within corporates, from small companies to large enterprise networks.

Citrix has been providing levels of remote access since 1989, first with their Multi-User OS2 terminal server. Following the success of Citrix-Multi-User, they went on to develop for the Microsoft Windows operating systems and the milestones include:

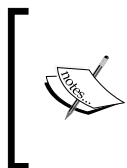
- 1993 – WinView releases
- 1995 – WinFrame releases
- 1998 – MetaFrame releases
- 2008 – XenApp releases

In the early days of WinFrame and MetaFrame terminal servers, you would have to provide some third-party **virtual private network (VPN)** solution to be able to access these servers from the Internet. In many respects, the weakness of these early solutions is that they do not address secure remote access.

To mitigate this issue, Citrix introduced a product into the market, in 2001, called **Citrix Secure Gateway (CSG)**. This is still available today and is bundled with XenApp 6.5. This, much in the same way as CAG, is a remote access solution that can be used to provide remote users on the Internet connectivity to your internal resources, such as your XenApp or XenDesktop servers.

Without CAG or CSG, each Citrix XenApp server and/or each XenDesktop virtual machine would require a public IP address to be accessible from the outside world. Of course, this is not practical, especially when we look at XenDesktop; do you have 300 public IP addresses available for your virtual desktops or VDI environment?

Both the CSG and CAG can act as an ICA proxy to provide connectivity to your internal Citrix servers.



ICA is the Citrix protocol for remote access. This can be listened on TCP port 1494 (for standard ICA connections) or TCP port 2598 (for session reliability). Session reliability tunnels ICA traffic through port 2598 to allow for momentary loss of connectivity, as would be experienced with mobile networks, and to allow seamless reconnection to the session.

So, if both devices can provide the ICA proxy functionality, why use CAG?

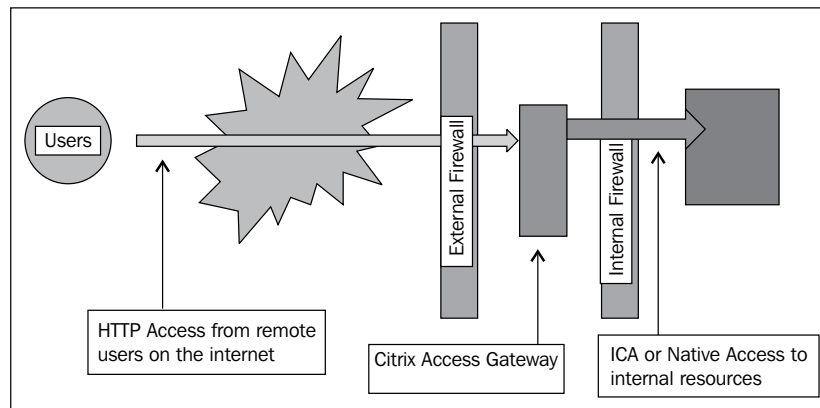
In 2005, Citrix systems acquired NetScaler, Inc. This gave them the NetScaler product range, and ultimately, Access Gateway. Quite simply, CAG is a secured system dedicated to remote access. It is supplied as either a hardware appliance or virtual appliance.

By "dedicated", it is meant that CAG has no other function, purpose, or unnecessary services. It is hardened or locked down for security at the time of production. CSG, on the other hand, is a software that installs onto a running operating system. We are, then, reliant on the OS that it is installed upon to be specifically hardened to provide the same level of security that you find out-of-the-box with CAG.

In addition to this, CAG can provide standard VPN connectivity into your private networks for remote users, not just connectivity to XenApp or XenDesktop. Choosing the appliance-based CAG includes support for additional applications and protocols. The software-based Secure Gateway is not only less secure but is also limited to supporting traffic directed to computers running XenApp or XenDesktop. Therefore, organizations that use the Secure Gateway might also have to deploy a remote access solution for other types of internal network resources, adding additional expense and management workload for already busy administrators.

CAG can handle your organization's remote access needs by securing traffic to applications hosted by Citrix XenApp and desktops hosted by Citrix XenDesktop as well as access to internal resources, such as e-mail, internal Web applications, and network file shares. In short, CAG is a secure remote access solution to provide VPN or ICA proxy access to internal resources to your mobile or remote workforce.

The following diagram illustrates that users connecting from the Internet pass through the external corporate firewall to the Access Gateway. From here, the incoming HTTPS is converted to an ICA stream targeting XenApp or XenDesktop servers. Possibly, even native protocols are converted to non-Citrix products when using a full VPN connection.



Citrix Access Gateway hardware

CAG, as mentioned already, can run as a virtual appliance or on physical hardware. The physical hardware device is a dedicated Citrix NetScaler appliance and comes in various shapes and sizes. The CAG firmware is installed into the NetScaler appliance, which runs an embedded Linux operating system. The same firmware that is used to run CAG on the hardware appliance can be used on the VPX edition, for example, both the VPX appliance and NetScaler 2010 model run Access Gateway 5.x firmware.

NetScaler Model 2010 Appliance

Model 2010 Appliance represents entry-level dedicated hardware and supports Access Gateway 5.0 and Access Gateway Standard Edition. In this book we will focus on Access Gateway 5.0.4. You can install Model 2010 in the DMZ or the secure network. The preconfigured IP address of the Access Gateway is 10.20.30.40. Citrix will tell you that you are able to change the IP address using a serial cable and a terminal emulation program such as Microsoft Windows Telnet Client, or you can connect Access Gateway using network cables and Access Gateway Management Console in Access Gateway 5. Usually, connecting via the network to change the IP address is the simplest method; just ensure you are plugged into a non-production environment when making the change, and then switch the appliance back into the DMZ. The following is a screenshot of NetScaler MPX 5500 Appliance model:



NetScaler Model MPX 5500 Appliance

This model boasts multiple processors, and from that, you can gain faster throughput and more concurrent connection support. Citrix provides Access Gateway in multiple forms to suit your organizational needs. This model supports Access Gateway Enterprise Edition. The preconfigured IP address of Access Gateway is 192.168.100.1 with a 16-bit or class B subnet mask. The IP address is changed in the same way as Model 2010.

Other hardware appliances are available to support the growing amount of concurrent connections that you may require.

You can install the Access Gateway Enterprise Edition appliances in the DMZ or the secure network as with Access Gateway 5.

The main difference between the models is their hardware specifications. The higher the specification of the hardware, the more users the appliance will support, and it will be quicker in those tasks. One of the first tasks in the planning of your appliance is to answer the question "how many concurrent connections do we need to support?" or, simply "how many users will be connected to the appliance at the same time?".



If you are using VPX, the specifications can be managed by assigning fewer or less resources such a RAM and CPU to the virtual machine.

The following table conveniently lists each of the hardware appliances and their main specifications:

Appliance Specifications	2010	5500
Processors	1	1 dual core
RAM in GB	1	4
Power supplies	1	1