Building Your Complete Remote Access Infrastructure on Windows Server 2012

Windows Server 2012

Iron Networks White Paper
August 2012

Introduction

Remote access is a complex challenge for IT administrators. Providing system access to remote users involves a broad set of technologies including security, advanced networking challenges and support for a variety of end user devices including home PCs, laptops, tablet computers, PDA computers and smart phones.

The access technologies described in this include providing access to:

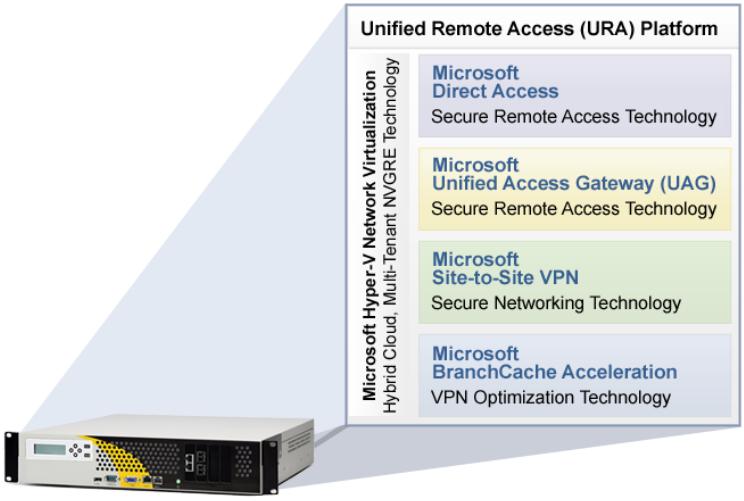
- Remote Managed Devices – Microsoft DirectAccess provides support for corporate computers attached directly to the Internet but also joined directly to the corporate domain and administered under Active Directory and other corporate management systems including Systems Center.
- Remote Unmanaged Devices – With the Windows Server 2012, computers not managed by the corporate IT department can be used to access corporate resources securely. These remote computers are insecure, such as home PCs also accessed by non-employees or other mobile devices including tablets and consumer devices, but Windows Server 2012 provides a method to secure these devices and provide a secure remote access solution.
- Remote Sites – Corporations often have multiple locations and these remote sites can be connected to the corporate network using various WAN technologies. To create a network WAN between sites via the Internet, some form of VPN is typically used. This document describes three scenarios:
    - Site-to-Site VPN – These remote sites are connected via Site-to-Site VPN devices which provide similar services as remote sites connected via leased line technologies.
    - Branch Sites – Iron Networks provides extended capabilities over standard Site-to-Site which includes WAN Optimization, Network Virtualization and network service extensions to the branch locations including Read Only Active Directory services, DHCP, DNS, and others.
    - Clustered Desktop Networks – This scenario is for smaller offices which have no Site-to-Site VPN services, but has a small number of desktop devices, each network attached to the corporate office directly using DirectAccess and BranchCache technologies from Microsoft.

Iron Networks packages and pre-integrates a broad set of technologies into a family of appliances. The Iron Networks product family is the Unified Remote Access (URA) product line running on a Windows Server 2012 platform. These products remove most of the challenges and complexity of providing a broad set of advanced remote access services and provide a plug-n-play appliance experience.

Unified Remote Access

The Unified Remote Access Appliances are based on Windows Server 2012 Hyper-V and can run multiple virtual machines. Each virtual machine can run different remote access technologies including

- Microsoft DirectAccess
- Microsoft Unified Access Gateway
- Microsoft IPsec VPN Services
- WAN Optimization technologies from Iron Networks
- Microsoft BranchCache for network acceleration of DirectAccess and Iron Networks Branch Appliance technologies

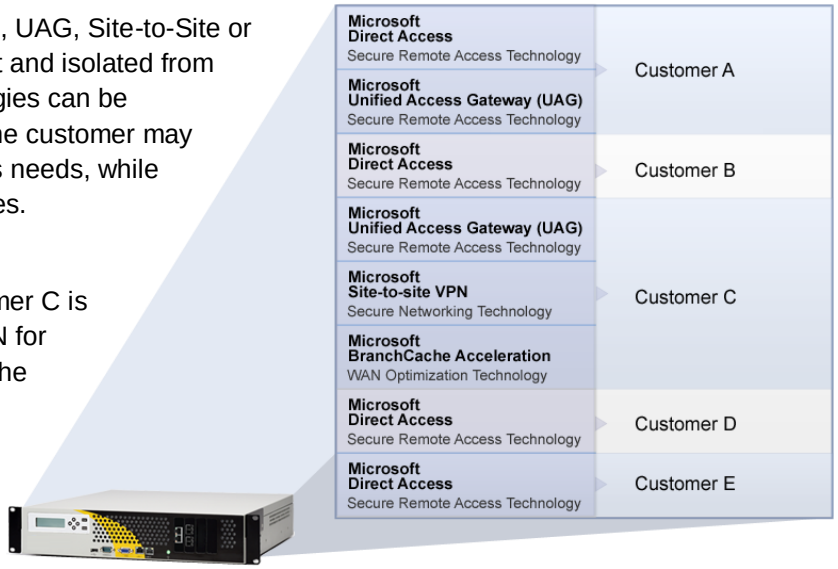


Each Unified Remote Access product can be configured with one or more remote access technologies, providing the flexibility to support just the technologies desired, or adding additional remote access technologies when desired.

Multi-Tenancy - Support multiple customers with a single appliance

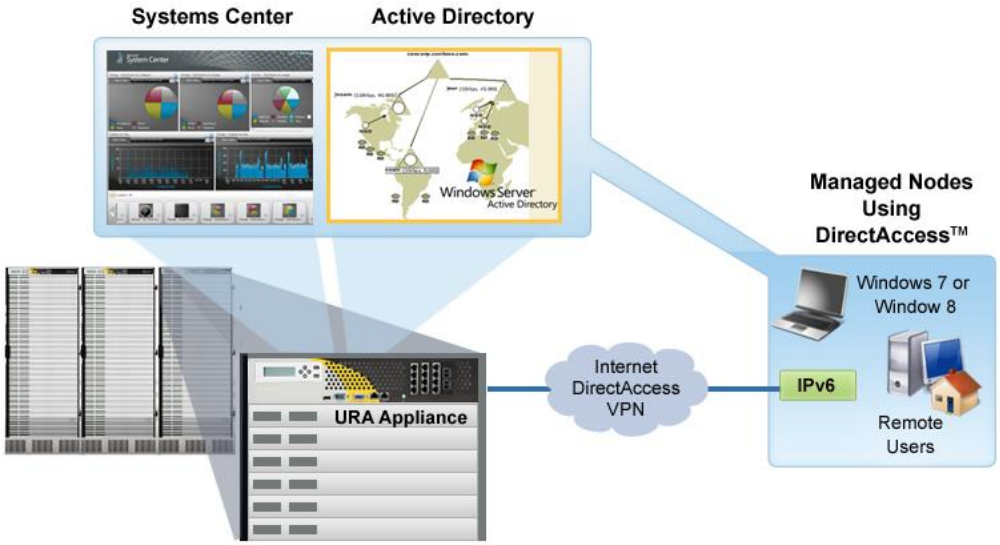
Since each virtual machine running DirectAccess, UAG, Site-to-Site or other remote access technologies is independent and isolated from other customer tenants, remote access technologies can be dedicated and isolated to specific customers. One customer may only require DirectAccess for their remote access needs, while others may desire a broader range of technologies.

In the example diagram, Customer B is running DirectAccess only for remote users, while Customer C is utilizing UAG for mobile devices, Site-to-Site VPN for their larger locations and Branch Appliances for the smaller remote site locations.



DirectAccess- Managed Remote Desktops

Microsoft DirectAccess™ provides a remote access solution for corporate computers that reside at remote locations such as user's homes small remote offices. These remote systems are centrally managed using the standard management technologies used by IT departments to manage local computers. Remote computers are under the control of Active Directory and managed by Systems Center or other management tools.



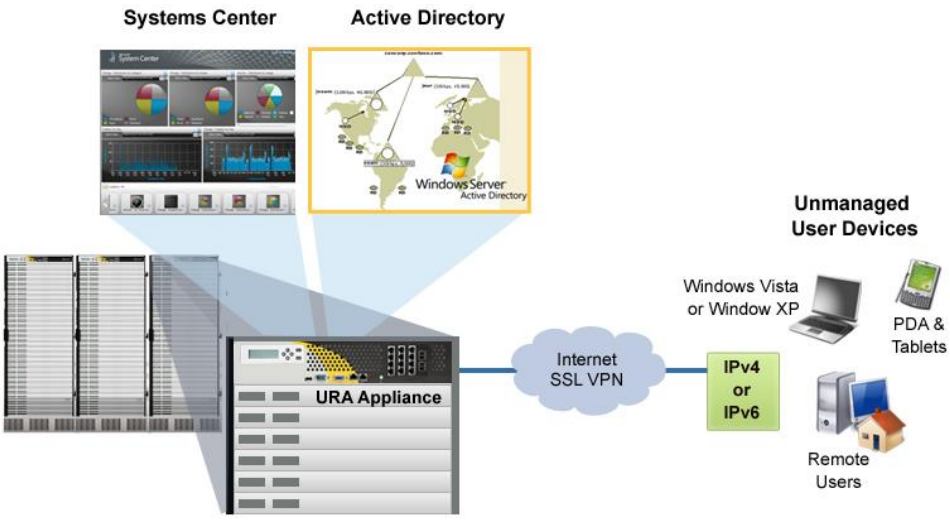
DirectAccess is the ideal remote access technology for extending corporate networks to remote Internet attached locations. DirectAccess end computer management includes Active Directory GPO policies, patch management via Systems Center Operations Manager or other systems, internal DNS, CIFS network shares, and all management provide centrally by the IT Department.

The Iron Networks Unified Remote Access appliance adds additional technologies to the DirectAccess feature sets including:

- Hardened Appliance Features for extended security required for Internet facing traffic
- Security Firewall add-on using Microsoft Forefront Threat Management Gateway to protect the corporate network from Internet threats
- FIPS 2/3 Compliance and HSM (Hardware Security Module) features for high security installations
- Integrated Multi-Factory Authentication using the Gemalto Digital Security technologies. These include Security Tokens, PKI Smart Cards, and others
- Off-Premises provisioning to allow remote computers to join to the corporate Active Directory domain from a remote location
- Remote Access for Windows-to-Go ™ computers. Windows-to-Go is a Microsoft technology which is an entire Windows 8 operating system contained on a USB stick. A remote user can connect his USB stick to a foreign and insecure computer and boot from the USB stick. Once booted:
    - The user is running a complete Windows desktop, completely isolated from the host PC
    - The Windows-to-Go system can be domain joined and immediately connected to the corporate domain and access all resources allowed by his Active Directory credentials
    - The Windows-to-Go system can also be protected by the Gemalto Digital Security system, where if the user were to lose the USB Windows-to-Go system, an additional factor such as a token or smartcard would be required to access corporate resources.
- WAN Acceleration for DirectAccess remote nodes using the Microsoft BranchCache™ technologies. BranchCache is included with the Iron Networks Unified Remote Access appliance, and provides faster and more reliable access across an Internet connection.

Unified Access Gateway (UAG)- Unmanaged Desktops and Mobile Devices

Iron Networks has built in Microsoft Unified Access Gateway 2010(UAG 2010) on a virtualized instance on the Windows Server 2012 Platform. One of the great features of Windows Server 2012 Hyper-V is that it allows you to run any service, on any server, in any cloud. In taking advantage of the virtualization capability of Windows Server 2012, Iron Networks was able to build in the older UAG 2010 technology to provide additional remote access capabilities on the appliance. The Microsoft Unified Access Gateway (UAG) 2010 provides reverse proxy publishing of remote user access to corporate services such as Outlook, Lync, SharePoint, any Web Based service and most client/server based services in a single web portal.

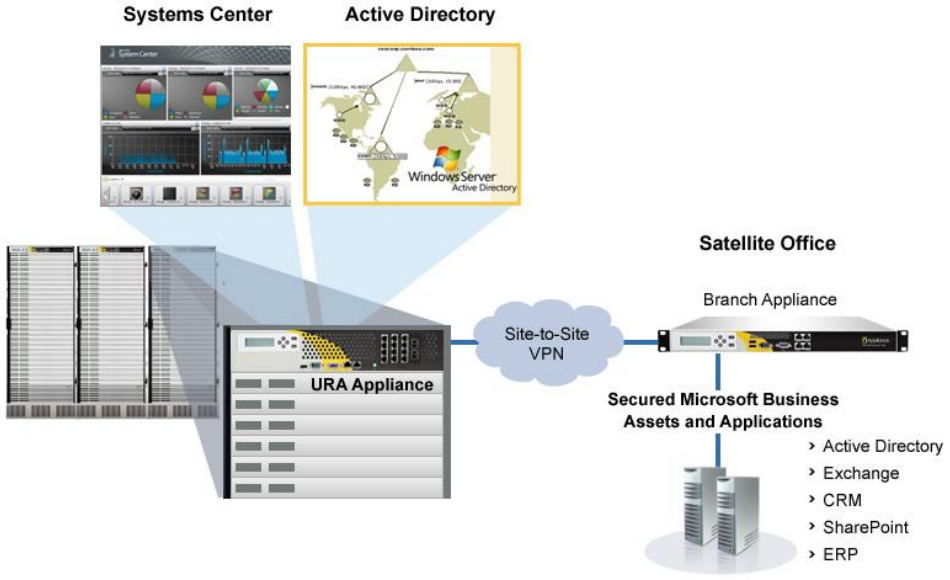


UAG 2010 provides endpoint protection and interrogation, where an end user computer must pass the corporate access policies before access is allowed. This provides an easy to use remote access solution through a web browser, all enabled on top of the Windows Server 2012 platform.

The combination of Windows Server 2012 DirectAccess and UAG 2010 portal publishing provides a comprehensive remote access solution.

Site-to-Site VPN- WAN networks over the Internet

The Iron Networks URA appliance includes a complete Site-to-Site VPN solution set. This technology requires a hardware device on both ends of the Internet, and the Iron Networks URA appliance works in conjunction with the Iron Networks Branch Appliance to provide a secure WAN solution.



The Site-to-Site VPN links corporate sites and are commonly deployed as WAN backbone links. When combined with routing protocols, VPN circuits can be deployed in mesh networks.

WAN circuits based on shared networks such as the Internet can have unpredictable performance and reliability. Network technologies such as WAN optimization and QOS are an important part of the solution for a Site-to-Site VPN product.

The URA Appliance includes the following features:

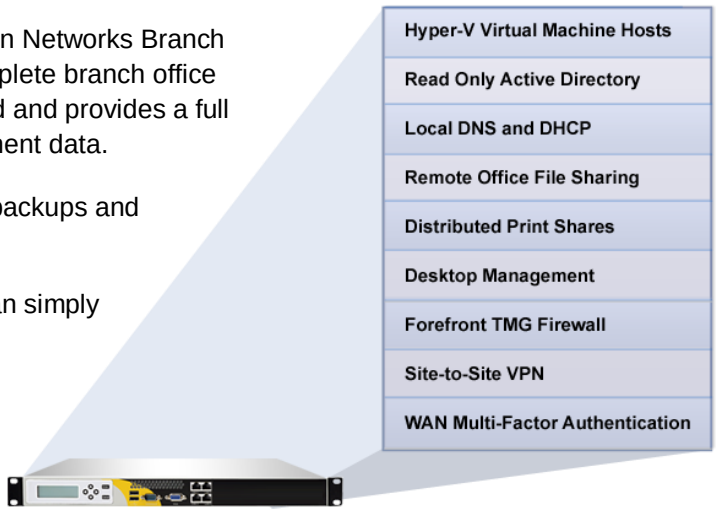
- Hardware offloading of IPsec protocols
- 10 Gig Network Interface ports
- WAN Optimization technologies for IP protocols
- BranchCacheWAN Optimization technology from Microsoft
- Hardware performance tuned for high-throughput network circuits

BNA: Branch Appliances- Branch Office in a Box

In addition to advanced VPN network technologies, the Iron Networks Branch Appliance includes a set of services which provides a complete branch office solution. The branch office appliance is centrally managed and provides a full set of IT services for remote offices without storing permanent data.

Since no permanent data is retained, the requirement for backups and critical system management is removed.

Branch appliances that suffer failures or physical abuse can simply be replaced similar a typical network appliance.



The software features of the Iron Networks Branch Appliance include:

- Hyper-V Virtual Machine Hosts – each branch appliance is based on Hyper-V and has the capability of running additional virtual machines. Customers can run their own software instances to meet custom business requirements.
- Read Only Active Directory – Active Directory queries such as logins and GPO processing is processed locally at each branch location, speeding up the performance for branch users.
- Local DNS and DHCP – DNS and DHCP processing is also processed locally at the branch location.
- Remote Office File Sharing – Microsoft DFS file sharing and share replication greatly enhances the branch location network and overall performance.
- Distributed Print Shares – Print shares can be extended for printing from corporate office servers down to branch locations.
- Desktop Management– Desktop management systems are included in the software stack of the branch appliance. Desktop management is the largest IT overhead and source for helpdesk phone calls.
- Forefront TMG Firewall – The Microsoft enterprise firewall is included so the branch appliance can securely face the Internet and maintain corporate security.
- Site-to-Site VPN – Enterprise and feature rich Site-to-Site VPN is included as described above.
- WAN Optimization – Enterprise and feature rich WAN Optimization technologies are included as described above.
- Gemalto Multi-Factor Authentication – Enhanced access security is gained by using Multi-Factor authentication using tokens or smart cards. Gemalto the leading provider of token and smart card technology, and is the branch appliance is seamlessly integrated with the Iron NetworksGemalto appliance solutions.

The Branch Network Appliances tightly integrated with the product solution sets from Iron Networks, Microsoft and Gemalto and provides a complete IT solution for small to mid-sized branch office locations.

Summary

The Unified Remote Access solution from Iron Networks that is built on the Windows Server 2012 platform, includes seamless integration of a stack of technologies including firewall security, multi-factor authentication with networking technologies including SSL VPN, Site-to-Site VPNs to provide a remote access technology which encompasses individual users on individual mobile devices in a BYOD environment, to managed corporate laptops, to full office installations at satellite branch locations all running securely on Microsoft remote access technology.

Iron Networks, Inc.
980 Mission Court, Fremont, CA 94539, USA
Phone: +(1) 408-895-5000 (Local), +(1) 877-895-6277 (US-Toll Free), +(1) 408-895-5000 (International)
Fax: +(1) 408-943-8222/8101 Email: info@ironnetworks.com Website: www.ironnetworks.com