Mobility's Impact on Remote Access

13 February 2013 ID:G00236637

Analyst(s): Phil Schacter

VIEW SUMMARY

Mature secure remote access infrastructure is adapting to changing mobility use cases, device types and ownership models, and to support authorization based on rich context.

TABLE OF CONTENTS

CONTENTS

ACRONYM KEY AND GLOSSARY TERMS

ACS	Access Control Server
AD	Active Directory
ADC	application delivery controller
ASA	Adaptive Security Appliance
BYOC	bring your own computer
BYOD	bring your own device
DMZ	demilitarized zone
DVPN	dynamic virtual private network
IaaS	infrastructure as a service
IKEv2	Internet Key Exchange Version 2
IMC	Intelligent Management Center
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISE	Identity Services Engine
ISR	Integrated Services Router
MDM	mobile device management
NAC	network access control
NAT	network-address translation
NCP	Network Communications Products
NLB	Network Load Balancing
OTP	one-time password
PCoIP	PC-over-IP Technology
PKI	public-key infrastructure
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
RIM	Research In Motion
RRAS	Routing and Remote Access Service
SDI	Server and Domain Isolation
SDN	software-defined network
SGT	security group tag
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	single sign-on
UAC	Unified Access Control
UAG	Unified Access Gateway
URAS	Unified Remote Access Service
VAN	Virtual Application Network

VDI	virtual desktop infrastructure
VM	virtual machine
VPC	virtual private cloud
VPN	virtual private network
WAN	wide-area network
WLAN	wireless LAN
WPA2	Wi-Fi Protected Access 2
XACML	Extensible Access Control Markup Language

Summary of Findings

Bottom Line: A mix of secure wired, wireless, virtual private network (VPN) and server-hosted virtual desktop infrastructure (VDI) technologies is needed to support new and expanded use cases for remote and mobile access. Multiple advanced policy systems will need to coexist, with few industry standards to support interoperability and enable consistent policy enforcement.

Context: Today, many organizations are pursuing strategies to enable mobile work from any device, from any location and at any time of the day. Changes in use cases, mobile work patterns, and the demand for secure remote and mobile access solutions are influencing policy changes, investments in upgraded infrastructure, and short-term changes in IT network, application and security architecture. Looking ahead, the expected enterprise use of hybrid private and public cloud services, accessed over a mix of public and private networks, involving Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), wireless LAN (WLAN) and cellular networking protocols, and an even more diverse set of managed and unmanaged devices, will require multiple approaches for secure connectivity.

Take-Aways:

- Secure remote or mobile access requirements have evolved beyond traditional "road warrior" use cases that only focus on external access from remote locations, company-provisioned laptops and use of two-factor authenticators.
- New and extended use cases include support for partners, work-from-home programs, bring your own device (BYOD) programs, secure access to a remote cloud provider and support for access to a consistent workspace image while roaming.
- A mix of IPsec and Secure Sockets Layer (SSL) VPN gateways continues to be widely used for use cases that each is well suited for, with the SSL-based approach providing the greatest flexibility for a range of use cases involving nonemployees or access from devices not provisioned by IT.
- Secure connectivity solutions come in hardware and software appliance form factors, and are often delivered as a component of a multifunction network or security platform offering.
- Secure access and connectivity services are provided by network infrastructure, wireless network infrastructure, virtualization infrastructure, application delivery controller, network security, and solutions that implement platform- or application-specific secure protocols.
- Enterprises face significant challenges in assuring the identity of users and devices, while providing the convenience of single sign-on (SSO) for access from a growing range of portable computing devices.
- Secure networking based on IPv6 and software-defined network (SDN) approaches are still mostly for early adopters.
- Microsoft's DirectAccess and an improved Unified Remote Access Service (URAS) make it easier to deploy and operate on hybrid IPv4 and IPv6 networks, but for most clients, the Microsoft solution and the industry's support for IPv6 and transitional protocols need to mature.
- Long-term planning for investments in secure access infrastructure needs to consider expected changes in use cases, a diverse set of endpoint devices and ownership models, and an architecture that accommodates multiple technical approaches and hosting models.
- In the short term, customers will often need to use several solutions to satisfy their use cases. Although these solutions can provide advanced context-based access control, their policy management is by and large solution-specific.

Strengths:

- Established remote access vendors are innovating and investing in expanding their capabilities to support secure access for a broader mix of mobility use cases.
- Some BYOD program risks can be mitigated by secure access mechanisms that are able to identify and segregate unmanaged endpoint devices.
- Mechanisms that intermediate access between the requesting endpoint and the target service create a clear point for access policy enforcement and the creation of a reliable audit trail for satisfying compliance audits on which users (and devices) accessed which services and associated regulated data.

Weaknesses:

- Current industry standards are not sufficient to ensure consistent policy across multiple technical access enforcement mechanisms.
- Mechanisms that authenticate and establish a secure connection for accessing IT services and data generally involve a trade-off between usability and security — this is especially true for the latest generation of touch-based endpoint devices.
- Application silos are re-emerging independently as mobile applications address the need to authenticate, authorize and establish secure connectivity to the back-end application infrastructure.

Recommendations:

- Take an architectural approach to addressing the expected classes of use cases and avoid ad hoc solutions to unanticipated secure access requirements.
- Seek versatile solutions that can evolve rapidly to keep pace with a faster innovation cycle for consumer-oriented technologies and products.
- Build capacity, within the secure access infrastructure for future usage and business continuity scenarios, that enables rapid expansion in the number and types of endpoint devices that can be supported.
- Be agile and accommodate diversity in the technologies and endpoint devices that internal clients are likely to require. Consider segregating newer types of devices until their risk level is better understood or additional controls can be deployed.

Conclusion: Secure access to IT services by diverse endpoint devices will require a mix of technical access policy and enforcement mechanisms, as determined by the use cases that need to be addressed. It will also involve traditional VPN suppliers and other technology partners that natively support secure network and application layer protocols.

Table of Contents

Analysis

As IT markets emerge and solutions mature to address a relatively stable set of use cases and requirements, products converge on a set of features. Purchasing decisions tend to be swayed more by the buyer's relationship with the vendor or channel partner. The secure remote access market has been going through such a maturation process for most of the past 15 years. Several recent trends and new or expanded use cases have a disruptive effect, causing established vendors to innovate, develop or acquire new capabilities to meet them. The most important trend prompting this market response is the integration of employee-owned consumer devices that are highly portable, intended to operate on wireless and cellular networks, and that create security, device management and application management challenges for the enterprise. Secure remote access and secure mobile access infrastructure solutions are converging, as established vendors respond to client and market needs.

Table of Contents

Evolution of Remote Access

Today, many organizations are pursuing strategies to enable mobile work from any device, from any location and at any time of the day. The remote access infrastructure required to support secure mobile work not only includes the latest generation of hybrid VPNs (supporting IPsec and SSL), but also use of secure wireless controllers, SSL to secure internal Web portals and other secure protocols that connect to a server-hosted virtual desktop (SHVD) (Remote Desktop Protocol [RDP]), a Unix/Linux system (secure shell [SSH]) or that are specific to another application system. While the traditional remote access use cases persist and still need to be supported, other types of mobile work do not require a VPN, and may not even be classified as remote access if the accessing device is situated within a secure facility or campus environment.

Secure remote or mobile access is more broadly defined as:

> A set of secure communication protocols and infrastructure that enables confidential, bidirectional, exchange of data between an authenticated end-user computing device and one or more infrastructure devices that enforce policy governing access to restricted information and application systems.

Typically an access-initiating endpoint consists of an identifiable user using an authorized portable device to access a set of permitted application and network services. Remote or mobile access may also have the context of the device's geographic or network location, whether it is managed or unmanaged, and additional risk factors (such as behavior over time, device configuration and a real-time assessment of whether the device is running required security software and patches).

Table of Contents

Historical Context for Remote Access

In the earliest days of mobile work, remote access involved dial-up, points of presence and modem pools. Since the late 1990s, remote access programs have focused on VPN technologies that establish a cryptographically secure tunnel over the public Internet, connecting an agent installed on the remote computer to a VPN gateway inside the private network firewall. Over the past several years, many organizations have adopted clientless SSL VPNs that do not require network-address translation (NAT), and that provide more advanced policy systems that limit which internal applications and servers the mobile worker or external partner can access.

Table of Contents

Traditional Use Cases

The most common use case is the so-called road warrior — a frequent traveler (knowledge worker, including sales professional) provisioned with a company-managed laptop. As laptop prices declined, even white-collar employees that travel only rarely are now being supplied with a company-managed laptop that can be easily taken to conference rooms, to another company facility or for occasional work from home.

Many organizations are also expanding their full-time work-from-home (or telecommuting) programs, providing participating workers with a company-managed laptop, and either VPN access or a connection to the extended WAN. Often, a different approach is taken for occasional work-from-home, where a limited set of services can be accessed from an employee's home PC over a public Internet connection, typically as an SSL session, with secure servers located in the demilitarized zone (DMZ) or between the Internet-facing firewall and the internal network's inner firewall.

Unexpected peaks in occasional work-from-home demand often occur during regional storms, during spare-the-air days and in a variety of business continuity scenarios where access to a primary work location is not recommended. Prior arrangements with remote access infrastructure vendors can provide flexible licensing for this kind of "surge" in demand, but additional hardware capacity will be required, or it will need to be possible to add capacity with minimal delay.

Remote vendor support may require a specialized service that is able to limit access to the specific systems that need to be supported. Some form of terminal server (or server-hosted virtual desktop) or monitored SSH session is often used to satisfy this requirement.

Table of Contents

Characteristics of Remote Access and Mobile Access Programs

Remote access programs tend to be managed by the network operations function, with a primary focus on maintaining availability. They typically involve a fault-tolerant configuration of multiple VPN appliances, with sufficient capacity to deliver a slightly degraded level of service to most users during a fallback scenario. Additional configuration flexibility may be needed to provide access during periods of unexpected high demand, such as during regional storms or other business continuity scenarios.

As the number of mobile devices supporting wireless networking proliferates, the number and capacity of internal and guest wireless networks needed to enable access from company facilities also grow. As a result, some organizations now maintain three distinct WLANs for guest (visitors, including vendor personnel and some contractors), internal (company-managed devices only) and, most recently, in support of BYOD programs. Each WLAN has its own unique set of security requirements and, therefore, tends to be segregated to specific public, internal trusted and limited access security zones.

Whenever a mobile device is considered to be outside of the trusted perimeter or is not fully trusted as a managed device, then selective access to internal services requires the use of a secure protocol, and an application or gateway mechanism for establishing identity and evaluating authorization policies.

Table of Contents

Driving Change in the Near Term

For many organizations, changes in use cases, mobile work patterns, and the demand for secure remote and mobile access solutions are already influencing policy changes, investments in upgraded infrastructure and short-term changes in IT network, application and security architecture.

Table of Contents

New or Expanded Use Cases

The assumption that most work requiring access to IT services is performed by an employee using an IT-managed Windows computer from a secure company facility is no longer valid for many organizations.

External Access by Nonemployees

For a variety of global business reasons, there is a growing set of requirements to provide limited access to internal IT services by partners, outsourced IT development and support centers, external call centers, vendor support and other contractors. These external, nonemployee use cases typically leverage the VPN gateway, terminal server or SHVD as the mechanism for enforcing access policy and limited access to specific IT assets.

Work From Home

Many organizations now support full-time and part-time work from home, and see strong growth in participation in such programs. This work flexibility is attractive to workers and the business, reducing demand for expensive dedicated office space in favor of shared hoteling facilities to support home workers when they visit a company facility.

There is also further blurring of the workday boundary as a result of always-on mobile devices that regularly sync to corporate email. Restrictions on access from employee-owned home PCs align with other programs that enable the use of employee-owned computers and tablets.

Employee Device Ownership

An overwhelming trend is for employees to acquire the latest consumer technology and, subsequently, find ways to leverage these devices for work due to their ultraportability and improved UIs. In addition to the usual Apple smartphone and tablets, enterprises are starting to see more Android devices and, in the short term, should expect an influx of consumer devices from Microsoft and OEMs that run a variant of Windows 8. Organizations are maturing their policies and programs to deal with the access requirements and facilitate community support forums for consumer devices that are not managed and supported by IT.

Securing Hybrid Cloud Workloads

One of the more recent use cases for VPN technology is to provide a secure network connection between the private corporate network and one or more cloud infrastructure as a service (IaaS) providers, so that virtual machine workloads can be securely moved between internal and external hosting data centers. Such a service may be offered as a virtual private cloud (VPC) or as a virtual instance of the VPN gateway software running at the cloud provider's site.

▲ Table of Contents

Expanded Mobility Programs

Mobility programs are rapidly expanding their capacity and capabilities in response to business demand for the flexibility to roam and to access IT services from any location.

One Person Accessing Services From Multiple Devices

For many organizations, knowledge workers rarely have to share a PC. Now, in addition to the company desktop or laptop, the user often has a smartphone that is enabled to synchronize with the company email and calendaring environment, and a tablet computer (at this point, typically an iPad), that can access email and a limited set of other business applications and services. Each of the user's devices may establish connectivity to IT services in different ways involving the internal LAN or WLAN, an external hot spot or guest WLAN, or an external 3G/4G cellular network connection via the public Internet. The security controls will need to vary to match the situation and the set of services the user needs to access.

Endpoint Diversity

The assumption that the user's device is a PC running a company-managed Windows image is less likely to be valid. Employees now often have a choice of smartphones from Research In Motion (RIM), Apple and one of the many suppliers of devices running Google's Android OS. Smartphones running Microsoft's Windows Phone OS may soon fall into this category. For organizations with BYOC programs, the user's PC may be an Apple MacBook or MacBook Air, or an Ultrabook that's not running the corporate Windows image. In the near future, the employee-owned PC may be running a variant of Windows 8, well before it is officially supported by IT.

The most likely third or fourth device the user brings to work and travels with on a regular basis is the tablet computer. One of the four generations of Apple's iPad is the most common tablet currently in use by employees, but compelling and more affordable Android-based tablets are also growing their presence in the market. The first generation of Windows 8-based tablets, including Microsoft's own Surface product line, are just entering the consumer end of the market, and will likely appear as another variant of employee-owned mobile device that needs access to some IT services.

Secure Wireless Networks

In many cases, mobility involves the use of public wireless hot spots, home wireless networks and guest wireless networks. Such networks cannot be assumed to be secure and, therefore, a VPN or other secure protocols are needed to protect the integrity and confidentiality of any business information transmitted over such a network. For internal wireless networks that are protected by the Wi-Fi Protected Access 2 (WPA2) protocol, there is no requirement for a VPN, with the wireless controller providing support for the authentication process and enforcing any required access policies. BYOD devices are generally segregated into a limited access security zone, which may require use of a VPN to access specific internal systems, regardless of whether the BYOD or guest WLAN is using the secure WPA2 protocol.

"Follow Me" Desktop

A growing number of organizations are pursuing a strategy of hosting virtual desktop images on data center servers and shared storage systems. Often, a nonpersistent desktop can be accessed from a generic device in any office location, or from mobile PCs and tablets that can establish network connectivity. For more information on trends in virtual desktop deployments, see "Desktop Virtualization: Building a People-Centric Infrastructure," "Decision Point for Desktop Transformation: Virtual, Physical or Server-Based Computing?," and "Peer Practices: Security Impacts and Benefits for Virtual Desktop Projects."

Scaling the Mobile Access Infrastructure

As the number of users that require remote, wireless and mobile access grows, the infrastructure that supports that access activity must also scale. Wireless networks will need to have the capacity to support more concurrent sessions and a different mix of data types that consume bandwidth, such as video streaming (where there is a business reason to do so). New or upgraded wireless access points may be needed at primary company facilities and, potentially, at many distributed offices or sites as well.

VPN gateways, terminal servers and server-hosting virtual desktops will need sufficient resources to meet user expectations for service levels and the increased peak demands.

▲ Table of Contents

Deployment Trends

A number of trends are already well under way in mobile access infrastructure deployments by enterprise organizations. Gartner field research on mobility and remote access deployments is more fully described in "Field Research Summary: Supporting Remote and External Access," "Field Research: Mobility in the Age of Consumerization," and "Field Research Summary: Mobility and Security."

Replacing Aging IPsec Gateways With SSL VPNs

The remote access solution for the managed Windows laptop that requires access to a broad range of internal network services has largely been an appliance supplied by a network or network security vendor that implements the IPsec and Internet Key Exchange Version 2 (IKEv2) protocols governing key exchange, authenticated Layer 3 connections and, optionally, encrypted session content. These solutions have now been on the market for 15 years, and older boxes from Nortel (now part of Enterasys), Checkpoint, Cisco and Juniper are now being replaced by newer offerings from the same or alternative vendors.

Often, the replacement is an SSL VPN capability that's one of multiple functions supported by a network or network security appliance, delivered by Cisco, Citrix, F5, Juniper and others. In addition to not having to deal with product-specific client software, since SSL VPNs offer an agentless option, these products avoid issues related to NAT and offer a range of access policies that can restrict the specific systems that the user can connect to. As such, SSL VPNs are much better suited to the new requirements for limited access involving nonemployee and BYOD scenarios.

For even greater flexibility, some products fully support SSL and IPsec, leaving the administrator to configure the optimal type of connection for the level of network service access needed by each user and type of device.

Consolidating Gateways Into Fewer Boxes

The latest generation of application delivery controllers (ADCs) from Citrix and F5 are highly scalable appliances and, frequently, are configured in a high availability pair that replaces a load-balanced farm of less capable VPN gateways. Other network security vendors, such as SonicWALL and Checkpoint, have evolved highly parallel architectures and a capability to scale up to handle more concurrent sessions, while performing multiple security functions on the traffic, with less impact on network latency. For business continuity, a similar pair of access devices is typically deployed to major regional data centers and backup sites.

Reducing the Number of Suppliers

For various reasons, organizations have ended up with different VPN solutions for specific use cases, or as a result of corporate mergers and acquisitions (M&As). Again, the goal is to consolidate and support all or most use cases with a single solution and, ideally, a single vendor relationship. The goal is to achieve reduced complexity, a lower total solution cost and a simpler environment to operate and administer. Rather than embrace smaller vendors, the enterprise buyer generally prefers to deepen its relationship with an established vendor that already provides it with other network or security services.

Securing Access to Virtual Desktops

Access to virtual desktops from remote and/or mobile devices leverage the Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA) or PC-over-IP Technology (PCoIP) protocols and, for some use cases, may not require a secure transport protocol. However, organizations that have security concerns due to publicized vulnerabilities in RDP (such as CERT's CVE-2012-002) may prefer to have users that are accessing their virtual desktops from a remote or mobile device first establish a secure VPN session. Remote access clients from VMware (i.e., View Client) and Citrix (i.e., XenDesktop and Receiver) operate over any secure VPN connection. Citrix provides additional integration within its NetScaler Access Gateway for adaptive access control and to provide single sign-on (SSO) capability. VMware View also provides SSO through its View Security Server role and integrated SSL VPN. Similarly, Array Networks has integrated its DesktopDirect mobile device application with its virtual and appliance-based Secure Access Gateway offerings.

Securing Access to SharePoint

Many organizations are looking for a way to securely publish some of their internal SharePoint content to authorized users accessing this content from remote or mobile devices. Microsoft Forefront Unified Access Gateway (UAG) has closely integrated its SSL VPN with SharePoint and its authorization model. Most other VPNs support SharePoint as they would any other internal Web portal. Mobile devices also can leverage native applications, such as Infragistics' SharePlus, that expose many of the features of SharePoint, while integrating with mobile device management (MDM) vendors for secure application distribution and container-based security functionality (for example, Good Technology).

Authenticating Remote and Mobile Users

Mobile workers, especially when using an employee-owned Ultrabook, tablet or smartphone, are unlikely to have access to the kind of one-time password (OTP) hardware token or smart card that organizations customarily require remote workers to authenticate with. Executive users and others are looking for a simpler approach that is consistent with the user experience of the device. When such devices are granted very limited access, the device is locked, requiring a PIN/password, and is subject to remote wipe after a reasonable number of failed login attempts (i.e., six to 10). The risk to the organization of a lost or stolen device being used to access IT services is relatively low. However, there are still use cases involving access to sensitive information and IT services that will require a multifactor authentication mechanism, regardless of whether the access originates from a company provisioned or employee-owned device. For more information refer to "Decision Point for Identity and Access Management in Mobility Projects" and "Decision Point for Authentication."

▲ Table of Contents

Technology Trends

Secure remote and mobile access programs are also benefiting from ongoing technical improvements and innovations.

User Transparent Connectivity

Organizations want to provide their users with a consistent network experience that is independent of device and location. Rather than the user having to explicitly start an agent or script that establishes a secure session back to the edge of the internal network, the goal is for the network connection to be transparently and automatically established, whenever the device is in operation. This is the promise of Microsoft's DirectAccess that most enterprise clients find compelling.

Similarly, Cisco's AnyConnect and Juniper's Junos Pulse can be configured to automatically connect using an available network and protocol, subject to cost-weighting factors established by the administrator. The user experience is intended to be transparent to the user, regardless of whether the device connects to the LAN, WLAN or to a VPN gateway. The exception to auto-connect occurs when the user and device are roaming and the available network is a "costed" connection, such as a 3G or 4G cellular network, with a hefty roaming surcharge.

Agentless Versus Intelligent Multifunction Agents

The promise of SSL VPN technology is that in most instances it eliminates the need to install client software on the mobile device in favor of transient code that runs within the browser. The transient agent is ideal when providing limited access to partners or from employee-owned home PCs and laptops/Ultrabooks, where you can't require the installation of specific software on a permanent basis. However, it does mean that some advanced functions may not be available, such as having native intelligence on the device to choose the lowest-cost connection type, or to provide local configuration and security posture information that may be required for evaluation by the network device that grants access.

For mobile iOS and Android devices, the VPN vendor provides a downloadable "free" application through an approved app store. Cisco is currently in the process of integrating its CleanAccess agent with AnyConnect to work with the advanced version of the Identity Services Engine (ISE) as a network access control (NAC) policy system for enforcing some configuration and security posture requirements.

Virtual Software Appliance

The VPN gateway market began as a software market, with each instance supporting 100 or 200 concurrent connections. It then migrated to hardware appliances that eventually scaled out to support 10,000 to 20,000 concurrent connections. Now that data centers and public cloud IaaS providers have built up a virtualized computing infrastructure that can respond dynamically to peaks in demand, the focus is again shifting to the software appliance form factor. VPN vendors are starting to offer their gateway as software that can run as instances in one or more virtual machines. For example, Array Networks has a virtual version of its Secure Access Gateway and limits each virtual instance to a maximum of 6,000 concurrent sessions. The resources necessary to support the workload are defined, and then a cloud orchestration product determines how many instances to run. Service providers are billed monthly for actual usage, based on data gathered by a license server. Citrix NetScaler Access Gateway VPX and F5 BigIP Edge Gateway virtual edition are similar offerings.

Advanced Policy Systems

For many years, VPN gateway products simply relied on any available Remote Authentication Dial-In User Service (RADIUS) server to support the user authentication and access decision processes. However, as policy systems become more advanced, they go well beyond the RADIUS standard. To support the more advanced functions, you need to match the vendor's VPN gateway, with its associated policy system. This is clearly the case with the latest Cisco Adaptive Security Appliance (ASA) appliances that leverage the advanced functions of Cisco's ISE, and are increasing their support for Cisco's proprietary security group tags (SGTs).

As users move between wired, wireless and VPN connections to the network, there is a growing frustration with variations in the access policy that may result from multiple policy systems. Vendors are moving toward a more consistent or so-called "unified" access policy, leveraging advanced policy systems that are shared across their product portfolios. Of course, this benefit only accrues if the network environment is sourced from a single supplier, or if there is a level of integration between the products and the rich policy system.

Single Sign-On

From the perspective of the user, a single login and authentication credential should satisfy the VPN gateway and the restricted internal service(s) that the user is connecting to access. Often, this is the Active Directory (AD) user identity and associated password. For the VPN gateway, achieving the SSO goal requires capturing the authentication data to pass on to a RADIUS server that integrates with AD for the initial validation, and then performing a proxy login using the same credential(s) to satisfy Windows Servers that require a Kerberos ticket.

Secure Application Access Portal and Workspace Aggregators

One of the roles of the VPN Gateway is to assist the user in identifying the set of applications that he or she is authorized to access, and navigating to the target system that's often located inside the DMZ's inner firewall. A customized Web menu of applications that the user can connect to is becoming an expected capability. The Gateway, as Application Access Portal, also provides a common place where access activity can be logged for audit and/or accounting purposes. It is also an intermediate point to proxy logins to the destination application as part of an SSO strategy.

More recently, workspace aggregator products have emerged that provide a consistent user experience, while facilitating SSO and access to a mix of internal and externally hosted desktop images and applications. For more information refer to referenced documents in Recommended Reading.

Managed Information Containers

A relatively new category of products establishes a managed and secure information exchange between a container on the mobile device and specific data center applications and information repositories. A secure channel is put in place that uses SSL between the container and a gateway that's typically located in the DMZ at the edge of the enterprise network. For more information see "Using Managed Information Containers to Protect Information on Mobile Devices."

ADC as Platform for VPN

ADCs are another class of multifunction network and security appliance that combines traffic management, application-aware traffic optimization, inspection of traffic for security policy enforcement and filtering, with an integrated SSL VPN capability. Both F5 Networks, with its BigIP platform, and Citrix with its NetScaler platform, are becoming popular choices as highly scalable SSL VPN appliances. For more information see "Application Delivery Controllers."

Application-Aware Software Defined Network (SDN)

Citrix recently announced (in early October 2012) an application control layer (Layer 4 to Layer 7) for its NetScaler SDX platform. Predefined templates, configurations and policies are provided for the most common applications and use cases, and can influence the SDN's configuration at Layer 2 and Layer 3. Applications are already being actively profiled and recognized by next-generation firewalls and intrusion prevention appliances, and leveraging this application context when making decisions about the network services that need to be logically configured is an important next step.

What Role Does IPv6 Play?

Internet Protocol version 6 (IPv6) offers the potential for authenticated and confidential communication between any user device and any target network-connected server/system, without the need for VPN gateways, NAT or tunneling protocols. However, the global transition to IPv6 is a long, slow process, and it's unlikely that Internet Protocol version 4 (IPv4) will ever be fully retired, at least not in our lifetimes. While the Internet is now carrying a mix of IPv4 and IPv6 traffic, most internal networks are still supporting only IPv4. Current network-based monitoring and traffic inspection tools are generally not yet able to correctly process the encapsulation headers that are used when transporting IPv6 packets over IPv4 networks. While network infrastructure vendors support native IPv6 protocols in their most recent products, many enterprise networks are running heterogeneous networks, with many network devices from a variety of suppliers and at different stages in their operational life, and with different levels of compatibility for IPv6 and hybrid (Version 6 through Version 4) v.6-v.4 traffic.

Scenarios for Layer 3 Secure Protocols

SSL VPNs have proliferated in enterprise networks, primarily as a more flexible solution for the growing population of nonemployee users and employee-owned devices that are not managed by IT. SSL has major advantages in not requiring a permanent software installation on client devices, relying on browser-loaded transient agents and enabling content inspection by terminating, and then cascading the SSL tunnel at an intermediate network device (such as a secure Web gateway). However, for some security-conscious organizations, the potential for confidential information to be exposed at an intermediate device or via an SSL man-in-the-middle attack is sufficient to revisit the future role for the IPsec or Layer 3 VPN.

For IT-managed Windows devices that can join an AD domain, there are group policies that can be used to establish a security association between the client device and a specific Windows server or logical grouping of servers (a domain), leveraging native Windows support for IPsec and, a feature that Microsoft refers to as Server And Domain Isolation (SDI).

Table of Contents

Vendor Strategies for Secure Access

There is no single vendor that dominates the enterprise market for secure access solutions. The IT infrastructure is no longer a near monopoly of client devices and servers running Windows, connecting over a network running just Cisco switches, routers and wireless controllers. However, collectively, as vendors innovate to compete, they are constantly raising the bar, providing enterprise buyers with new variations on how to identify, authorize and deploy secure connectivity for traditional and emerging use cases. Several vendors contributed insights into this look ahead at the near-term-future road map for secure access.

Microsoft

While Microsoft has never been considered a leading provider of secure connectivity services to the enterprise, it natively supports IPsec, IPv6 and SSL protocols at the Windows client and server. Although not widely adopted, SDI enabled a Layer 3 secure connection between Windows clients and Windows Servers, subject to rules established through Active Directory and Group Policy. With Windows 7 and Windows Server 2008 R2, Microsoft introduced its new DirectAccess feature for "always on" secure connectivity. While many enterprises embraced the concept, few were willing to tackle the IPv6 early adopter issues and transitional protocols that were required to deploy DirectAccess over their existing IPv4 networks.

Microsoft has substantially addressed the early operational issues with DirectAccess through enhancements delivered as part of Windows Server 2012. A new Unified Remote Access Service (URAS) feature combines the DirectAccess Server with the Windows Routing and Remote Access Services (RRAS), adds built-in NAT64 and DNS64 translation services, and support for a simplified deployment using a Kerberos proxy and Domain Controllers, rather than an internal public-key infrastructure (PKI). With the new URAS, a higher availability configuration is enabled through built-in support for Windows Network Load Balancing (NLB). Microsoft states that:

> Windows Server 2012 includes DirectAccess and RRAS VPN to provide secure remote access for Windows and cross-platform clients, and site-to-site VPN to support cross-premise cloud access.

While URAS has addressed many of the operational and configuration challenges with wide-scale use of DirectAccess, it still relies on IPv6 and transitional tunneling protocols that are not well supported by many network security products. One of the supported transitional tunneling protocols carries the required IPv6 payloads over IPv4 networks, using the industry standard HTTP-S protocol. Some larger enterprise clients are considering supporting a mix of Windows 7 and Windows 8 clients running DirectAccess that connects to a load-balanced set of servers running URAS as an alternative to traditional VPN appliances.

Microsoft acquired Whale Communications, and continues to offer the Forefront UAG as an SSL VPN software product and through OEM partners, as a hardware appliance. According to Microsoft, "Forefront UAG will focus specifically on secure application publishing and cross-platform SSL VPN access for a range of mobile device." While UAG has had some success with large enterprise customers, especially as part of an integrated solution to provide secure access to internal SharePoint environments, it relies on OEMs to complete an appliance solution and to integrate its various tools into a deployed solution.

The market has changed as the Windows PC was joined by tablets from Apple and others in enterprises, depending on the business use cases for portable computing devices. While Windows 8 Pro tablets are able to join a Windows Kerberos domain, most other tablets and non-PC mobile devices will not be able to do so, and will therefore be unable to take advantage of DirectAccess (note: DirectAccess requires a Windows Enterprise license). Within two to three years, a maturing DirectAccess capability, with its always-on secure connection, is likely to be adopted by many of

Microsoft's enterprise customers, although it will be only one secure access mechanism in the portfolio of technologies needed.

Network Infrastructure Vendors

Most enterprises have a major investment in Cisco network infrastructure as well as products from competitors offering Layer 2 switches, wireless controllers, traffic management, RADIUS server-based policy systems and VPN gateways. For many Cisco customers, secure connectivity is provided through Cisco's ASA 5500 appliances or through VPN services integrated with a Cisco Integrated Services Router (ISR). Cisco provides a clientless SSL solution as well as its AnyConnect Secure Mobility Client for Windows, Mac OS and Linux-based devices. There are AnyConnect client versions for Apple iOS and Google Android mobile platforms. AnyConnect also integrates with Cisco's Web Security cloud-based and appliance offerings.

Cisco's ISE is the advanced policy system and RADIUS server offering that mostly replaces Cisco's Secure Access Control Server (ACS) product, while supporting Cisco TrustSec-based security groups, dynamic device profiling and additional context-based access authorization decisions. While ISE is still maturing, it promises to provide a consistent policy for access decisions across wired, wireless and VPN connections, as claimed in Cisco's October 2012 announcement of Cisco Unified Access. In particular, ISE's device profiling capability is able to identify and segregate unmanaged BYOD or guest devices.

Juniper Networks is a long-term secure networking partner for many enterprise clients, based on its SSL and IPsec VPN appliances, and supported by its Unified Access Control (UAC) policy system. Junos Pulse software provides an integrated client agent for endpoint devices to establish a secure connection and enforce NAC-style posture-based policies. Following its 2010 acquisition of SMobile, Juniper expanded its Junos Pulse offering to include a suite of endpoint security features and MDM functionality. Juniper is moving in the direction of an integrated policy solution for secure access across all devices and types of connectivity to the enterprise IT environment.

HP offers its dynamic virtual private network (DVPN) for IPsec-based secure WAN connectivity, with VPN policies managed by Intelligent Management Center (IMC). HP's strategy for the software-defined network is based on an application-aware framework, the Virtual Application Network (VAN) and its OpenFlow-based SDN controller as part of a larger HP FlexNetwork architecture. HP also supports access policy through IMC and the IMC User Access Management Module, enforced by HP infrastructure.

Virtualization Infrastructure Vendors

While, traditionally, we haven't relied on server virtualization vendors for robust access security solutions, the dominant role of virtualization infrastructure in cloud and mobility solutions is mandating more attention to secure access, SSO and advanced policy systems. Citrix is adding Zenprise (MDM vendor) to CloudGateway mobility management and secure access solution — built on its NetScaler platform and Access Gateway technologies. NetScaler SDX is the foundation for Citrix, supporting the software-defined network and enforcing access and traffic policies that are aware of application layer context.

VMware's vCloud Networking and Security 5.1 (incorporates vShield) provides a mechanism to segregate workloads within a virtual data center, leveraging emerging network virtualization technologies and a supporting policy system. It also includes an Edge Gateway (virtual appliance) that combines firewall and VPN functionality. Fine-grained access policies are administered through vShield Manager.

Other Secure Networking Vendors

The secure access market also intersects with wireless network infrastructure solutions from vendors such as Aruba Networks, application delivery controllers from Citrix and F5 Networks, integrated firewall and VPN offerings from Checkpoint Software and others and niche VPN providers such as Network Communications Products (NCP) Engineering. Vendors, for which secure network access capabilities are intended as complementary to products from network infrastructure vendors, understand that their solutions need to leverage industry standards, such as RADIUS, and offer some value-add that improves the operational and usage characteristics of their respective solutions when deployed in the enterprise network.

For the smaller niche vendors, their business success is largely dependent on the stand-alone value of their secure access and connectivity products, and related services and client support. For larger niche vendors, the strategy tends to be providing integration with their other networking or security offerings, along with a shared policy system and management tool.

▲ Table of Contents

Planning for the Long Term

The secure access solutions that worked for the heavily managed endpoint over the past decade are still performing well for similar use cases, but they are insufficient for most organizations to address the more diverse set of devices and risk scenarios that have emerged over the past several years. Today's diverse user device, device ownership, use case risk profiles and application hosting models require a blend of secure networking protocols and mechanisms. Looking ahead five or perhaps 10 years, the enterprise use of hybrid private and public cloud services, accessed over a mix of public and private networks, involving IPv4, IPv6, WLAN and cellular networking protocols and an even more diverse set of managed and unmanaged devices, will require multiple approaches for secure connectivity.

Wherever possible, the preference will be for end-to-end secure exchanges between mutually authenticated sending and receiving parties — the devices, users, applications and back-end services that provide access to information and IT-enabled business processes. Architectures that terminate the secure exchange at a gateway, Web portal site or intermediate IT services broker will still be needed, but they create a point of termination of the cryptographic protocols, exposing the content on the intermediate system and, potentially, on the rest of its network path to the requested service.

When creating an architecture strategy that intends to address the enterprise's needs for five to 10 years, you need focus on the logical functions and avoid binding your plans to a specific vendor's product road map. The long-term view requires vendor independence and the flexibility that industry standards provide.

Table of Contents

Policy System Paradox

Secure access control administration and enforcement mechanisms are dependent upon a policy system that is becoming more advanced and less able to constrain its functions to industry standards, such as RADIUS. As each vendor innovates and unifies policy creation, evaluation, and its runtime protocols and APIs, the policy system becomes a product in its own right. Such advanced policy systems may still support industry standards, but generally offer additional functionality when used with other products from the same vendor. In a sense, the most advanced and desirable "unified" policy systems are not interchangeable and devolve to a lower level of functionality when operating in a heterogeneous product environment that relies on industry standards.

The paradox comes in when you need multiple advanced policy systems, or prefer not to use the policy system that's most closely integrated with your network, virtualization or security vendor's broader product line. Clients are faced with the difficult choice of operating their Juniper VPN or Aruba wireless controllers, based on Cisco ISE's RADIUS functionality, or installing multiple native policy systems, such as Juniper's UAC or Aruba's ClearPass. In the short term, the most likely scenario is that policies will become exportable from one system in either a standards-based Extensible Access Control Markup Language (XACML) format, or as a vendor-defined file that can be further massaged prior to bulk importing consistent policies into policy systems from other technology partners. Longer term, network access policy systems will need to evolve to a level comparable to enterprise identity and authorization systems, and implement emerging standards such as OAuth (see "Enterprise Use Cases for Open Identity: OpenID and OAuth" and "Decision Point for Selecting Authorization Mechanisms").

Table of Contents

Strengths

While the vendor offerings and road maps are still evolving, there are some positive trends that benefit organizations with secure access requirements and diverse use cases.

Table of Contents

Vendors Are Embracing New Mobility Scenarios

The network and network security vendors that provide secure connectivity solutions see the business opportunity from new mobile devices, BYOD programs and access-from-anywhere roaming scenarios. Product lines are expanding through acquisition and focused investment in supporting secure connectivity and exchanges involving all the mobile devices that are important to enterprises.

Table of Contents

Solutions Mitigate Some BYOD Risks

Secure access offerings provide a mechanism for identifying unmanaged devices, authenticating the user and device, apply granular access policies that limit access by untrusted devices and ensure the integrity and confidential of information being exchanged while it's in transit. These mechanisms can be used as part of a limited access zoning strategy to segregate BYOD devices, enabling the organization to realize the worker productivity benefits while protecting internal IT assets.

Table of Contents

Forces Auditable Access and Compliance

By providing a mandatory mechanism that intermediates access to internal and potentially cloud-based applications, there is a clear point in the mobility architecture for auditing who is accessing what application, and from which device (and location). The resulting audit trail becomes important for demonstrating compliance to mandated access policies, and as a source for forensics data to support an incident investigation process.

Table of Contents

Weaknesses

The current and most likely future scenarios still rely on fragmented solutions, with undesirable characteristics.

Table of Contents

Many Suppliers and Few Standards

Secure access solutions for a rapidly evolving set of mobility use cases will come from established network infrastructure and network security vendors, and new vendors participating in the mobile platform ecosystem. To address a broad range of use cases, the enterprise will need to deploy multiple solutions that will operate independently, based on disparate policy systems. Current suppliers are not investing in interoperability or industry standards to ensure seamless coexistence and consistent policies between solutions that may be optimized for different common use cases.

Table of Contents

User Experience May Suffer

Secure access solutions may require the use of specialized mobile applications or software installed on the portable computing device that are used to create an authenticated and secure connection to IT-managed assets. This connection is rarely transparent to the user, and may involve multiple prompts or use of a two-factor authentication process. There is an unavoidable trade-off between usability and security, and mobile devices are not exempt. In scenarios that involve use of a virtual desktop that's hosted on an internal server, there's also a user experience trade-off in simulating mouse-like functions from devices with native touch-based interfaces.

Table of Contents

Application Silos Persist

Just as organizations struggled with application silos on other platforms, mobile devices are facing a similar situation for some of the familiar reasons. Each custom and commercial application seeks to operate independently of all others and, therefore, embeds its own authentication, authorization and secure connectivity features. When aggregating access to multiple internally and externally hosted applications from the mobile device, there may be multiple authentication events and associated credentials required. Establishing a form of SSO for the mobile user and device is an important strategy, but requires a common tool or API that will be consistently applied by custom and commercial app developers.

Table of Contents

Recommendations

For the foreseeable future, large enterprises will need to provide secure access for a mix of legacy remote access use cases and new scenarios involving secure access from mobile consumer devices to internally and externally hosted applications and data.

Table of Contents

Take an Architectural Approach

While it may be tempting to take a tactical approach to each access request, such a process is not scalable as the requests multiply from a handful to scores of them. A better approach is to gather requirements from internal and business unit stakeholders, and create an architecture that addresses the main categories of use cases. Such an architecture will not be dependent on a specific vendor's product offerings, and is likely to include a traditional VPN gateway, a server-hosted virtual desktop capability, one or more secure Web portals (including a broker that aggregates access to cloud-hosted services) and the use of other application layer secure protocols (as required). Keep in mind that the secure access architecture is not stand-alone, and will intersect with network perimeter and zoning architecture, mobility architecture, monitoring, malware defense, content inspection, identity and access management, and other enterprise security architecture decisions. The goal is to invest in a small number of standard access solutions that will address all or most of the access request variants, and to stop building ad hoc implementations as new requests come in.

Table of Contents

Seek Versatile Solutions

Products that solve a single problem may be highly optimized, but lack the versatility to deal with rapidly evolving use cases, new mobile platforms and a changing mix of applications/services. Products that are bound to a 12-month or longer update cycle will limit the enterprise from deploying the latest devices or supporting their customers with services that can be securely accessed from the latest consumer devices. Versatile solutions will feature more frequent software refresh cycles, perhaps three or four per year. If a hardware form factor is needed for scalability, then it should be capable of accommodating major feature enhancements, without requiring a hardware refresh cycle for at least several years.

▲ **Table of Contents**

Build In Capacity for Future Usage Scenarios

The population of portable computing devices that may require secure access to IT-managed assets is expanding rapidly. The few thousand mobile road warriors with enterprise laptops connecting to a VPN gateway are being augmented by line-of-business deployment of tablets, widespread use of smartphones as a secondary access device, and additional employee or partner-owned devices supported under a BYOD program. Instead of a single device or less than one device per employee, there is a likely scenario that each employee will have between two and four devices that will require some level of secure access. Where a legacy VPN may have supported a thousand concurrent sessions, the future secure access infrastructure may need to support ten times that level. Look for an architecture solution that can easily scale in response to increased demand and new use cases — perhaps an approach that runs additional instances of the software as virtual machines (VMs). Similarly, make sure vendors are providing flexible licensing options that allow for periodic peaks in demand and support disaster contingency planning.

▲ **Table of Contents**

Be Agile and Accommodate Diversity

Over many years, IT organizations have fought a mostly losing battle to constrain diversity in the technology and product choices of their internal clients and business units. The power of a centralized IT organization to limit the technical choices within business units of the enterprise is fading. Occasional resistance to such control is being replaced with decentralized IT and autonomous technology decision-making models. The choice of which mobile devices to provision to employees, and which employee-owned devices to allow to access IT services should be a collaborative effort that allows for a wide range of choices. It should be flexible in adapting to the rapid pace of change in the consumer-driven mobile device market.

Consider providing multiple levels of access that vary, based on the assessed level of risk associated with a class of mobile device. As additional security controls are put in place or the level of risk is reassessed based on real-world experience, then grant the device a higher level of access. For example, early Android devices may qualify for guest access only, while more recent and secure versions (i.e., running Android 4.x and an MDM agent) may qualify for a limited access zone along with other devices in the BYOD program. The goal is to avoid having to say no to new devices, but to manage the risk as you learn more about its security capabilities. Diversity in the devices that access IT services is a trend that will persist for a very long time, and IT needs to evolve to accommodate it to reduce friction with internal clients.

▲ **Table of Contents**