White Paper

The Pervasive Network Access Voyage

By:

Jon Oltsik
Enterprise Strategy Group

June 2007

Table of Contents

This ESG White Paper was developed with the assistance and funding of Juniper Networks.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

Executive Summary

Business managers see "high touch" benefits to network access and why not? Lots of organizations have increased revenue, lowered cost, bolstered productivity, and improved communications by opening network doors to guests, contractors, suppliers, business partners and customers. This access comes with a price however. The more endpoints and users that access the network the more dangerous the network neighborhood becomes. It's hard enough monitoring employees for behavior and endpoints, now IT is forced to do the same thing for outsiders with their own network devices.

Somehow large organizations must strike a balance between network access and security for internal and external users as soon as possible. This white paper concludes:

- **Network access needs continue to evolve.** A variety of users access the network through assorted networks, at diverse locations, through multiple devices. Continuing globalization, increased bandwidth, and smart devices will add further complexity to this mix over time.

- **The scope around enterprise network access can be daunting.** Faced with this complex matrix of access needs, networking professionals can quickly look like the proverbial deer in the headlights. Technical issues can be rapidly overshadowed by the fundamental question of where the heck to start.

- **Large organizations need pervasive network access.** Islands of point tools or isolated network add-ons are a short term fix at best. CIOs need to think in terms of an evolving architecture composed of network, security, and management technologies. With ever-changing business needs and a persistent increase in the number of network users, the pervasive network access architecture must be flexible, scaleable, manageable, and extremely secure.

- **Pervasive network access will rollout in phases.** Pervasive network access needs will change constantly so it is important to start slowly and grow over time through three phases addressing: 1) Risk mitigation, 2) Strong policy enforcement, and 3) Network authorization.

Since pervasive network access depends upon an architectural approach, technology selection should be based upon a vendor's ability to deliver enterprise coverage, open standards, and expandability. Juniper Networks is one vendor who fits these needs.

The Changing Needs for Network Access

It has only been 14 years but it seems like an eternity. In 1993, graduate students Eric Bina and Marc Andreessen developed the first version of the Mosaic browser while working as programmers at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign, unleashing a communications and investment revolution. Visionaries pitched a multitude of "paradigm shifts" while venture capitalists backed every company with a web site or forward-looking product pitch.

In the midst of this new age ga-ga however, the reality is that early Internet usage was extremely limited. Afraid of being left behind, many businesses put up static web sites and served up HTML pages while pioneers actually sold things over the web. Still, Internet conversations were underway with users accessing web sites. As far as employees go, the big decision 12 years ago

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

was focused on which employees actually needed Internet connectivity. Many organizations viewed the web as a luxury or a distraction but certainly not a necessity.

Fast forward to today and the Internet of the mid-1990s looks quaint by comparison. The Internet is now viewed as a global IP pipe providing ubiquitous any-to-any connectivity. Beyond web pages, Internet connectivity has enabled new ways of automating business processes and improving productivity with IP-based communications, collaboration, and applications.

As part of this transition, network access has morphed from a privilege to a necessity. With the rise of Internet-based business processes, business managers insist that networks be "open for business" to employees, business partners, contractors, consultants, customers, suppliers, and a host of others -- around the clock. Driven by these business requirements, networking professionals are on the hook to provide secure network access for:

- **A host of anonymous "guest" users.** "Guest" user is an amorphous term that describes any non-employee who needs network access. This person could be a sales prospect touring corporate facilities, an outside lawyer hired to review a new union contract, or the CEO's daughter visiting Dad during spring break. To meet these business requirements, wary networking professionals have to devise a way to provide easy network access across wired, wireless and remote networks without compromising security.

- **Remote workers.** With growing access to broadband networks many users eschew the office in favor of telecommuting from home. A recent CDW survey indicates that 44% of federal workers have the option to work remotely, up 6% since 2006. A total of 62% of federal agencies now have policies allowing telecommuting, up from 46% in 2006. In this instance the federal government is actually ahead of the private sector but as the practice gains wider acceptance, it is likely that telecommuting will become a standard employee benefit.

- **Mobile employees.** Even employees at the home office remain mobile. In 2006, more than half of all business PCs were laptops, equipped with onboard mobile technologies for WiFi networking support. Once tethered workers now roam from conference rooms to cafeterias and expect constant network access along the way.

- **The next wave of network devices.** The next generation of network endpoints will include PDAs, smart phones, and fixed-function devices in numbers that dwarf worldwide PC utilization. For example, all PC manufacturers combined will ship between 200 and 300 million PCs in 2007, roughly the same number of handheld devices ship in the first quarter of 2007 alone. As these devices gain intelligence and connect over 3G and WiMax broadband networks, they too will need a key to the network door.

Network access issues don't discriminate by company size, geographic location or industry type. A manufacturing contractor in China needs to provide network access to North American customers as a small community college in rural Arkansas needs wireless access points across campus for students, faculty, and administrators. The network can no longer be separated from the business itself so access must remain omnipresent and enduring.

Mapping Out the Requirements for Pervasive Network Access

Network access control seems like a simple model similar to the role of a barroom bouncer at a trendy metropolitan nightclub. In order to gain entry, patrons are stopped at the door, asked for some type of identification credential, and looked over to see if they meet house rules. Most

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

patrons will be admitted with little problem but some will be denied access because of identity problems (i.e. a fake ID) or turned away because of non-compliance (i.e. a tee shirted man is denied access because the dress code specifies the need for a collared shirt).

Network access follows a comparable pattern. Users are asked for identification and inspected for policy compliance before they are granted network access. Most will easily pass this test but inevitably some will fail. This is where this analogy falls apart however, unlike the orderly queue at an urban hot spot; network access requirements are complicated because of:

- **Heterogeneous users.** Pervasive network access must be able to check identity and policy conformance on a wide variety of system types. Windows PCs will continue to be the dominant endpoint device but even this means supporting Windows 2000, XP, and Vista while still allowing access for Macintosh, Linux, UNIX, and mobile devices. This situation will become even more difficult with the rise of more smart handheld devices.

- **Multiple network entrances.** Rather than one line at the front door, users need network access from a multitude of locations and networks. For example, Mary in sales logs on to the network through a wireless hotspot at Boston's Logan Airport while an application developer in Bangalore gets granular access to specific applications and data through an SSL VPN. Onsite corporate employees and guests often use LAN access within an enterprise. Somehow, the networking team must devise network access policies and technologies that can accommodate all of these individual needs.

- **Different networks and equipment.** To keep in touch with the office, a traveling executive may need access from trusted, semi-trusted, and untrusted networks in a single day based upon her flight plans and appointment schedule. Controlling access in each of these circumstances may depend on a potpourri of networking technologies such as web single sign-on software, SSL VPNs, or a local access control appliance.

Pervasive Network Access Must Be Married to Security

Business initiatives demand network access to users and devices across the globe. This presents a complex technical challenge but access alone is only half of the battle. To enable business processes AND protect valuable assets, pervasive network access must be accompanied by strong network security. To marry security with network access, CIOs must protect against:

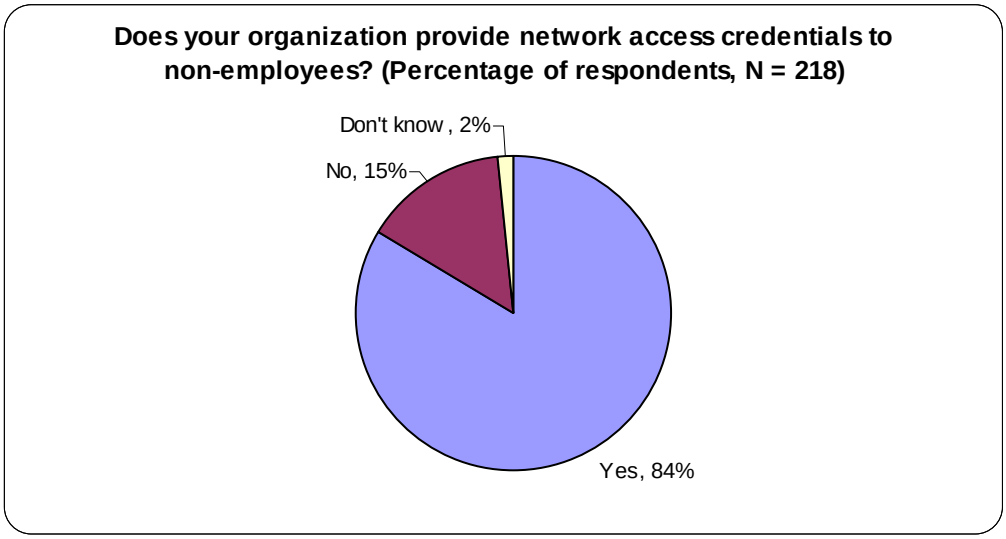
- **Unidentified network objects.** According to ESG Research, more than three-quarters of enterprise organizations provide network access credentials to non-employees today (see Figure 1). This will climb to close to 100% in the near future while the number of outsiders and devices needing network access will also rise. Trusting third party devices pose a real challenge for network security administrators when any single infected device could cause severe network damage.

- **Vulnerable endpoints.** To maximize network protection, software vulnerabilities must be patched in a timely and consistent manner. This process is hard enough with tethered desktop PCs, let alone a growing population of mobile devices and third party endpoints entering the network. Automated patch management helps remediate corporate PCs but doesn't help protect against sloppy external users or infected mobile devices.

- **Malicious code attacks.** While worm and virus attack threats have decreased over the past few years, researchers still worry about the next generation of "super worms" using multiple rapid propagation methods and containing highly destructive payloads. Obviously, a "patient zero" endpoint device could paralyze the network in a manner of minutes. To avoid this nightmare, proactive network-based security defenses must

become a network access requirement.

Figure 1. Most Large Organizations Provide Network Access to Non-Employees



- **Network snooping and hackers.** Even trusted users with clean devices could pose a problem if they start poking around the network, examining network assets and probing for weaknesses. In a perfect model, users would be granted restricted network access to the assets they need to do their jobs minimizing the risk of any insider trouble.

What's Needed? Pervasive Network Access

When it comes to security, large organizations often behave in a knee-jerk fashion. Users react to the threat du jour by implementing some type of technology safeguard. SPAM traffic begets SPAM filters. Spyware leads to the deployment of anti-spyware tools; and so on in a perpetual cycle.

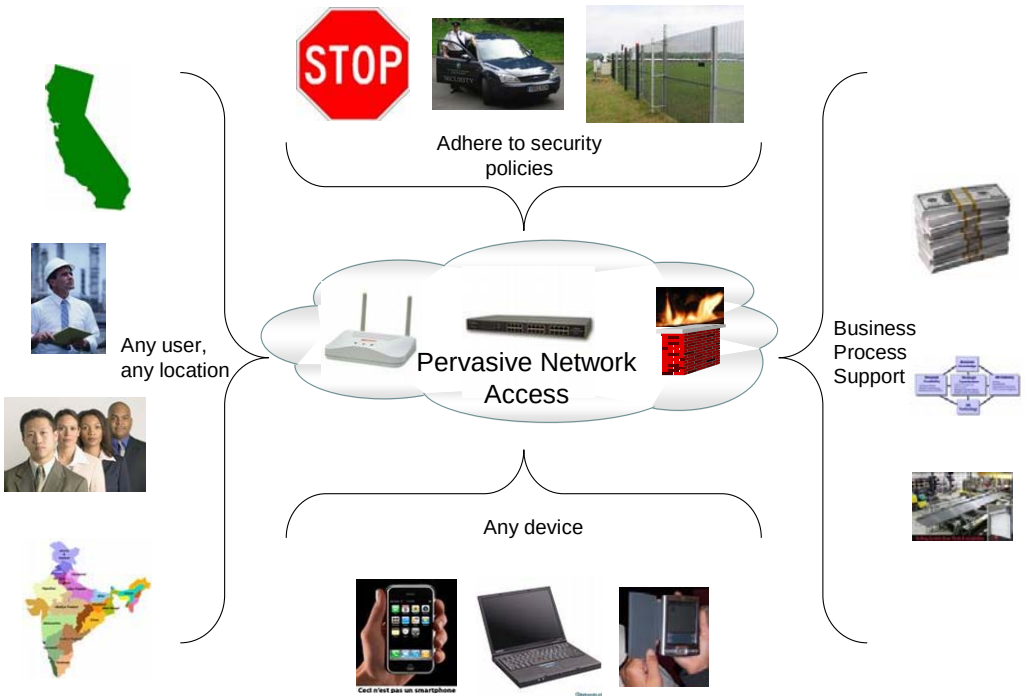
Enterprise requirements for network access follow a different path. Why? As described above, network access is fluid with lots of moving parts. Unlike other areas of security, there is no single technology solution; rather network access must combine multiple technology piece parts in an evolving architectural solution. Network access at large organizations must also accommodate a variety of users, endpoint devices, and business relationships. Network access decisions will vary based upon a matrix of questions about identity, device type, network location, time-of-day, etc.

ESG believes that CIOs must think in terms of a new model called Pervasive Network Access defined as:

A secure network access architecture that can be configured to enforce access and business policies across any mix of user roles, endpoint devices, and network technologies.

Parsing this sentence, pervasive network access is highlighted by its ability to support (see Figure 2):

Figure 2. Pervasive Network Access



- **User identity and roles.** Pervasive network access can be configured to make network access decisions based upon the business needs of internal and external users. A CFO, financial analyst, CPA and external auditor all need access to financial systems; pervasive network access can be used for access control and authorization at the network layer complementing identity tools and applications. An external auditor can be granted access to specific subnets, IP addresses, ports, and protocols while blocking passage to the rest of the network.

- **Business and security policies.** Pervasive network access starts with some elementary questions like, "what is the definition of a healthy endpoint," "which threats present the biggest threats," and "how should policies be enforced?" The answers to these questions will fluctuate from organization to organization and even user to user. Addressing these questions with sound -- and realistic -- policies may be the most important aspect in achieving pervasive network access success.

- **A combination of enforcement techniques.** It should be evident by now that pervasive network access enforcement must be adaptable to deal with a cornucopia of users, policies, and network edge technologies. When Susan the HR benefits manager accesses the corporate network from her local Starbuck's, she will receive different privileges than she will from her office.

Given the diversity in these three parameters alone, it is easy to see why so many IT professionals are confused or overwhelmed by network access decisions (see Table 1).

The Pervasive Network Access Architecture

The dynamic nature of pervasive network access must be addressed with an enterprise architecture including the network, security safeguards, management tools, and policy engines. The underlying architecture must be (see Table 1):

- **Flexible.** The pervasive network access architecture will have to have an exhaustive list of configuration options, network/endpoint device support, and integration choices in order to accommodate a matrix of users, policies, and enforcement methods. Since change is constant, this flexibility is crucial -- vendor lock-in or limited functionality may restrict business requirements down the line. The CEO won't be pleased when an HR outsourcing project has to be delayed because IT needs time to create 500 new accounts in Active Directory or reconfigure the network.

- **Based upon open standards.** Dynamic business requirements and network flexibility can only be achieved by building the pervasive network access architecture on a foundation of existing open standards such as RADIUS, 802.1X, SSL/TLS, and IPSec and the ongoing work of standards bodies like the Trusted Computing Group (TCG), IEEE and IETF. This is especially important for large organizations with existing heterogeneous networks and lots of different client types. Before buying anything, users should query vendors about their openness -- or lack thereof.

- **Manageable.** Pervasive network access flexibility calls for extensive deployment, configuration and policy options that can be easily administered and centrally managed. Management must extend beyond the network alone as various security (i.e. endpoint security, vulnerability scanning, log management) and operations management (i.e. configuration/asset management, software distribution, desktop support) play a supporting role. Check with vendors in each of these areas to see how they plan to integrate into industry frameworks like the Trusted Network Connect (TNC). At the very least, explore whether these tools provide open interfaces and standard logging formats.

- **Extremely secure.** The focus around network access has been on the "health" status of endpoint devices answering questions like: Are these systems patched? Do they have the right version of antivirus signatures? Yes, these are important issues but a single health check when users first log-in may miss endpoint compliance problems, suspicious user behavior, or a zero-day malicious code outbreak during run-time. To maintain network security, pervasive network access must perform periodic checks of endpoints, monitor user behavior, and actively filter packets to and from client machines.

Table 1. Pervasive Network Architecture Requirements

Requirements	Business Justification	IT Justification
Flexibility	Need to accommodate multiple user roles and business processes	Need configuration options for various policies and enforcement techniques
Open standards-based	Future needs are unpredictable but necessary	IT needs lots of options
Manageable	Business needs the ability to add and monitor users	Meet business needs with simple administration and auditing capabilities
Security	Enable business processes with minimal risk	Maintaining network availability while protecting critical assets

Unfortunately, meeting all of these criteria can be a tall order. Pressing business needs prompt many organizations to adopt network access point tools with limited functionality. The dynamic nature of pervasive network access almost guarantees that these tools will need to be replaced within a few short years. Taking a more architectural approach is the right strategy but many of today's solutions are built around proprietary standards and tools promising a future of vendor lock-in.

Juniper Networks offers an alternative to this no-win decision between point and proprietary tools with its pervasive network architecture. Juniper's pervasive network access architecture includes a comprehensive set of offerings suitable for enterprise deployments.

Juniper's product portfolio includes enabling infrastructure (i.e. 802.1X supplicants, RADIUS servers, and downloadable client agents), a policy management server (Juniper Networks Infranet Controller), and multiple policy enforcement technologies (firewalls, SSL VPN appliances, and 802.1X-compliant wireless access points). Juniper has also taken a leadership role in the Trusted Network Connect (TNC) group and maintains an extensive array of partnership with authentication software, PKI, and IT management vendors.

With its NetScreen acquisition in 2004, Juniper acquired its SSL VPN platform (formerly Neoteris) and has continued as the market leader since. With its focus on device inspection, granular access control, and the breadth of platform and device support, Juniper Networks Secure Access SSL VPN provides organizations of all sizes a flexible and scalable remote access solution - for mobile/remote employees, partners and customers – ensuring that these audiences see only what they are allowed to see. This helps to mitigate the risks of unmanaged devices or untrusted networks.

The Juniper Unified Access Control (UAC) solution has deep roots in its product portfolio. Juniper's SSL VPN product line can be seen as the progenitor of today's UAC. In its current rendition, UAC has combined internal development (i.e. Juniper Infranet Controller policy server, UAC Agent, NetScreen firewalls), acquisitions (i.e. Odyssey® Access Client 802.1X supplicant and Steel-Belted Radius® from Funk Software), standards (i.e. TNC, 802.1X), and industry partnerships (i.e. Microsoft NAP) into a flexible and powerful pervasive access control blend for LAN access. As such, Juniper's UAC strength may be its combination of centralized management along with a wide variety of enforcement points across the network.

In this way, Juniper Networks Secure Access SSL VPN and UAC product lines provide a pervasive network access solution for today's mobile enterprise.

A Pragmatic Approach to Pervasive Network Access

ESG recommends that CIOs take a pragmatic, measured and strategic approach to pervasive network access. Spend lots of time on upfront planning, working with business managers on policy definition, enforcement tactics, and preparing the organization. Monitor technical progress; help desk call volume and user reactions. Harden policies and enforcement over time but be sure to provide adequate services for users so they can remediate problems easily. Success depends upon understanding that pervasive network access projects and configurations will change and evolve.

Success depends upon a gradual implementation that builds through 3 phases (see Table 2):

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

1. Risk mitigation
2. Strong policy enforcement
3. Network authorization

Table 2. The Three Phases of Pervasive Network Access

Phase	Title	Business Objective	IT Objective	Benefit
1	Risk Mitigation	Enable a particular business process or user benefit	Identify and minimize security risk	Establishes pervasive network access experience while addressing a particular problem area
2	Strong policy enforcement	Eliminate security incidents to increase productivity and network availability	Increase security while automating IT operations	Users become self sufficient and more productive. Security incidence and IT operating costs decrease
3	Network authorization	Map business processes with user roles to accelerate business activities	Isolate traffic to protect valuable network assets. Ease monitoring and forensics.	Decreased cost/time of user provisioning. Improved business productivity and security.

Risk Mitigation

During its initial phase, pervasive network access should really focus on a particular high risk area. For example, the organization may have a large number of on-site contractors who need access to their own project management systems, collaboration tools, calendars, and email. Enabling this "guest" access would help accelerate the project and lower costs.

In this instance, IT managers should prioritize tasks around defining guest account policies, restrictions, enforcement methods, and monitoring user behavior. The project owner should take the lead to determine who will need network access for what purposes and work collectively with IT to characterize guest access policy requirements. IT teams will need to test solutions to make sure that guest users can easily follow instructions and network enforcement works the way it should. When guest access is rolled out to the contractor group, it is important to encourage user feedback, monitor network activities, and watch for curious user access patterns that may indicate malicious activities or technology problems.

Strong Policy Enforcement

In this second phase, IT should move beyond a small subgroup and take pervasive network access across the enterprise. This is where staging is critically important. IT should start by simply laying the foundation across endpoints and the network, monitor activities, and remain in a passive role. Users must be told that their endpoints will be inspected henceforth but that there won't be any other short term policy enforcement actions.

After a month or two in the background, IT should ease in a series of increasingly more stringent network access policies and enforcement responses. For example, initial policies may simply call for weekly antivirus signature updates. Over time, this policy can tighten to require the latest signatures and operating system patches. Enforcement should follow a similar trajectory. Initially users may be presented with an "out of compliance" message but no action. This should progress to a remediation grace period of 4 to 6 weeks. Enforcement periods should continue to decrease to days and finally hours.

It is critically important to deliver user training, clear and concise messages, and automated remediation tools as access policy and enforcement become less and less forgiving. When a user receives a pop-up message indicating that her laptop is considered "unhealthy," she should receive a clear description of the problem and given simple self-service tools for immediate remediation so she can fix the problem on her own and get back to work. ESG has found that disdaining these critical steps is a recipe for pervasive network access disaster. When users are denied network access without any clue about what to do, CIOs can expect to hear a cacophony of ringing help desk phones and screaming business managers.

Network Authorization

When endpoint health and remediation is sufficiently addressed, the next thing to consider is network authorization. This means mapping users, groups and roles to specific network subnets, VLANs, network assets, and applications based upon business needs and security requirements. For example, pervasive network access may limit guest access to an Internet gateway through TCP port 80 and 443, a financial analyst may be restricted to the finance subnet, and the VP of network engineering may have free reign across all devices and network segments.

Enforcing these kinds of access rules demands the full complement of pervasive network enforcement technologies from layer 2 through layer 7 implemented in a number of ways. Guest access restrictions may be enforced using firewall rules, the finance group could be controlled through a combination of network ACLs and VLANs, while wireless users are throttled by RADIUS servers and 802.1X.

As large organizations proceed through the second and third phase of this journey, pervasive network access should deliver a measurable ROI. Desktop and security incidents should decrease leading to greater network availability and utilization. Automated remediation tools should lead to more efficient device management at lower operating costs. Finally, the process for provisioning network accounts should be automated based upon user roles. In total, business utilization should go up while IT problems and operating costs head south.

The Bottom Line

Leave it to the technology industry to take a simple and necessary concept, spin it like a top, and confuse users. Thus far the discussion has been narrowly defined in a milieu of desktop security and network access controls with little mention of the wide array of business uses necessary. In truth, user roles, devices, network locations, and technology considerations must be considered in the context of who needs access to which network resources to accomplish what business task.

ESG believes that the matrix of business and technical considerations surrounding network access demands a more holistic architectural solution called pervasive network access. Pervasive network access mixes networking, security, and IT management into a flexible, scaleable, and manageable system. The objective of all of these pieces is simple – enable network business processes in a safe environment. Accomplishing this will take patience, time, practice and communications over 3 distinct phases as policies and enforcement rules are hardened over time.

As for technology solutions users should keep their guard up. Everyone is in this business and promising the moon. Look for open comprehensive solutions that can address immediate threats and then scale gracefully over time. Juniper Networks is one vendor that can meet these requirements.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com