

# The Future of Secure Application Access Management

A Netilla Networks White Paper



**Netilla Networks, Inc.**

347 Elizabeth Avenue

Somerset, NJ 08873

Phone: 732.652.5200

Fax: 732.764.8862

[www.netilla.com](http://www.netilla.com)

Part No.3.0.2.5.02 V 3.1.2.d5



---

## Table of Contents

|   |           |
|---|-----------|
| <b>INTRODUCTION: SSL VPNS AND THE BREAKING OF ENTERPRISE SECURITY .....</b> | <b>2</b>  |
| <b>SSL VPN'S: EXPRESS LANE INTO THE NETWORK'S CENTER .....</b>              | <b>2</b>  |
| <b>THE NEW PARADIGM: SECURITY POLICY ENFORCEMENT .....</b>                  | <b>3</b>  |
| <b>MARKET DRIVERS: ENVISIONING THE FUTURE OF SECURE NETWORK ACCESS.....</b> | <b>6</b>  |
| <b>PROVIDING SECURE APPLICATION ACCESS MANAGEMENT .....</b>                 | <b>7</b>  |
| <b>INTRODUCING NETILLA DYNATRUST™ .....</b>                                 | <b>8</b>  |
| <b>THE DYNATRUST ALLIANCE PARTNER PROGRAM.....</b>                          | <b>10</b> |
| <i>Symantec</i> 10  |           |
| Benefits of the Solution.....   | 10        |
| <i>WholeSecurity</i> 11   |           |
| Benefits of the Solution.....   | 11        |
| <i>Zone Labs</i> 11   |           |
| Benefits of the Solution.....   | 12        |
| <i>Sygate Technologies</i> 12   |           |
| Benefits of the Solution.....   | 12        |
| <i>Microsoft</i> 12   |           |
| <b>CONCLUSION .....</b>   | <b>13</b> |

## Introduction: SSL VPNs and the Breaking of Enterprise Security

Today's distributed, decentralized business environment demands open, flexible, and resilient access into the corporate network for a variety of constituents. These constituents, who may access resources from any number of locations, span the range of conventional business practices, and include contractors, vendors, partners, suppliers, road warriors, and employees. Ensuring that enterprise network resources are available for this diversified user base - from any location, at any time - has become a fundamental requirement of doing business.

In response to these needs, SSL VPNs have emerged as the vehicle of choice when extending authenticated network access to employees as well as organizational constituents traditionally considered "outsiders". The ease of use, fast Return On Investment (ROI), and plug-and-play simplicity of SSL VPN approaches - particularly when compared to traditional IPsec solutions - validate SSL VPN technology as the best way to deliver critical network resources to the remote business user, leading to genuine efficiency and productivity improvements.

Yet these advances come at a price: The exacerbation of enterprise security flaws. By its very nature, SSL VPN technology compromises traditional efforts to secure the network perimeter. This troubling consequence - shown in **Figure 1** - is due to the fact that, with SSL, users pass through the perimeter firewall on encrypted sessions that cannot be monitored by intrusion detection systems or inspected by firewalls. As a result, an unbridled troop of road

warriors, partners and telecommuters connect to corporate networks from a variety of unprotected endpoints, effectively bypassing the organization's perimeter security protocols. These unprotected endpoints include:

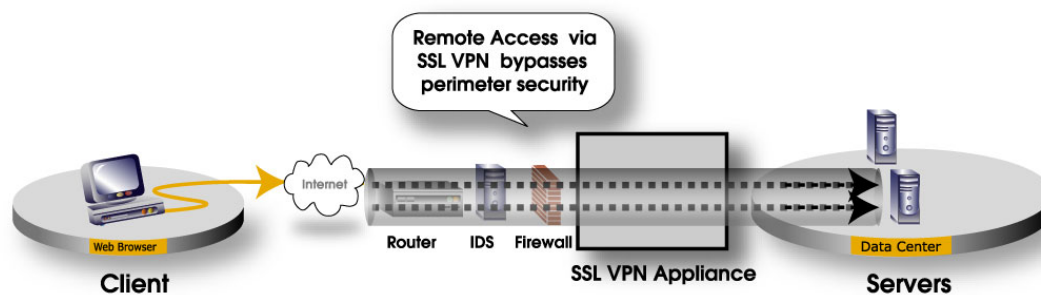
- Home PCs
- Remote networks belonging to an organization's customers and/or suppliers
- Wireless hot spots in airports
- Kiosks in hotel lobbies

This amalgam of unprotected endpoints represents the "nomadic fringe" of the network, providing hackers with an array of potential attack vectors to exploit what are essentially doorways into an enterprise network. The "nomadic fringe" represents the single greatest source of vulnerability facing chief security officers today.

This paper examines the threats brought by this class of network users, envisions the next stages for IP network development, and introduces the Netilla Networks dynaTRUST™ Operating System (O/S) as the policy enforcement point (PEP) solution necessary to overcome the security challenges associated with the nomadic fringe.

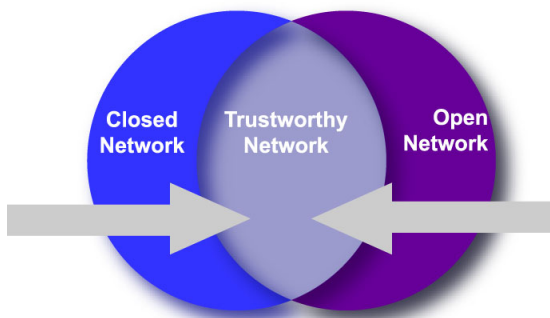
## SSL VPN's: Express Lane into the Network's Center

As the network's edge continues to expand and become more difficult to defend, conventional enterprise security methods are no longer sufficient. The advent of the SSL VPN has rendered obsolete the once-accepted practice of containing assets within a closed network and hardening the perimeter. A harsh reality of SSL VPN deployments is that the technology itself



**Figure 1: SSL VPNs Bypass Traditional Perimeter Defenses**

compromises once-accepted network security design conventions. **Figure 2** illustrates what had been the “best practice” security design paradigm, which dictates the establishment of trustworthy network zones to provide access to vital enterprise information resources. Characteristics of this security model are the use of Demilitarized Zones (DMZ), firewalls, security gateways, and intrusion detection systems that harden the closed network perimeter. However, containing enterprise information assets within a closed network is only effective when it is possible to both define the trust boundaries themselves, and police the entrants into the trusted network.



*Figure 2: Traditional Security Model*

SSL VPNs have broken this model. Rather than defining a hard perimeter, SSL VPNs provide authorized clients with an “express lane” to corporate information. SSL’s encrypted tunnels circumvent the conventional security measures that protect the closed network and thwart hacker access attempts. Yet an increasingly nomadic workforce, coupled with a growth in partner extranets, has made it impossible to segregate the internal network from the outside world. Trying to establish trust boundaries is futile in the face of the disappearing network perimeter. Hiding enterprise information assets within a hardened perimeter shell it is no longer a valid defense strategy. Consider, too, that the same user may today access resources from within the trusted network environment and tomorrow access the same information from a different un-trusted location. This is a critical scenario that must be understood in the new security paradigm brought by SSL VPNs.

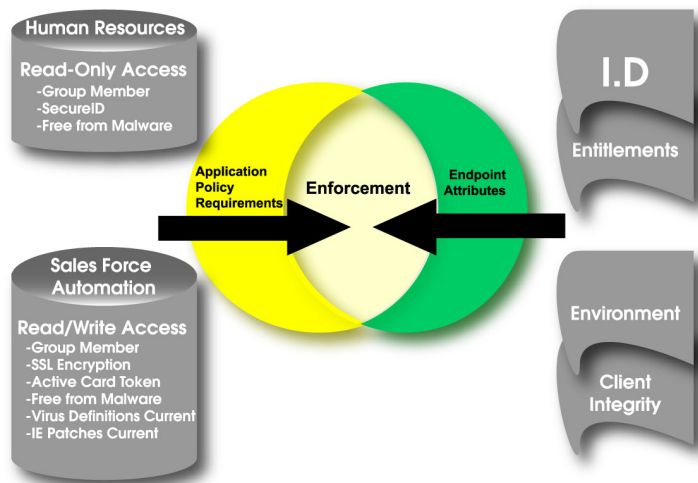
This blending of “insiders” and “outsiders” imposes a host of new security challenges.

Because PCs and laptops perform distributed processing functions, the remnants of a user’s activities can remain on the device. Viruses, Trojans, configurations that violate enterprise security policy, or rogue software all represent risk, particularly when the device deploying an SSL “express lane” connection is outside the scope of the enterprise’s control. Therefore, constant vigilance is required to protect the enterprise and ensure that the mobile workforce gains access to the corporate network in the most secure fashion.

Because all users typically have the same access privileges to sensitive resources irrespective of whether they are using a trusted to un-trusted node to access that information, the need to ensure client integrity is self-evident. The devices used to access enterprise information insert themselves as a trusted endpoint by default. Therefore, a compromise of the client device represents a sizable threat, providing hackers with an open doorway with which to launch an attack. Adequately mitigating vulnerability from the nomadic fringe mandates a new security design paradigm.

### The New Paradigm: Security Policy Enforcement

As a leading provider of SSL VPN technology, Netilla Networks understands that the concept of the closed network with a hardened perimeter must evolve into a Web of largely autonomous security domains - each protecting one or a few applications. Access for all



*Figure 3: The New Security Paradigm*

application users must be regulated by adherence to strict security policies. In this forward-thinking view, the protective network boundary moves from the external perimeter to the internal domains. The distinctions between internal or external, trusted or un-trusted, local or remote fade away as access control morphs from exception-case policies to fine-grained control applied to all applications. This new security paradigm utilizes strict policy enforcement to grant access to secure information domains. **Figure 3** illustrates this new paradigm, where applications publish their security policies and user access is granted as a function of policy compliance. Characteristic of this new security paradigm is the necessity to lock down all doorways by default and to only open doors as required, and then only to users or services that comply with the dictated security policies.

The Netilla Security Platform (NSP), an SSL VPN appliance from Netilla Networks, represents the first commercial offering of policy-based secure application access. From its genesis, the NSP's SSL VPN architecture has been designed as a Policy Enforcement Point (PEP), providing organizations with a vehicle to "enforce" strict access policies that control how and when a remote user gains access to an enterprise domain within the enterprise perimeter. Operating as a true application-layer proxy, the NSP provides secure remote access to both legacy and Web applications. To satisfy the need to lock down doorways by default, the NSP employs dynamic firewall functions that provision port-level services on demand. Dynamic firewall functionality is augmented by Netilla's SecureRealm™ architecture, which integrates authentication, authorization, and policy building blocks to control access on an individual, role, or group basis. Netilla's security policy enforcement approach to granting remote access differentiates the NSP from rival

SSL VPN products.

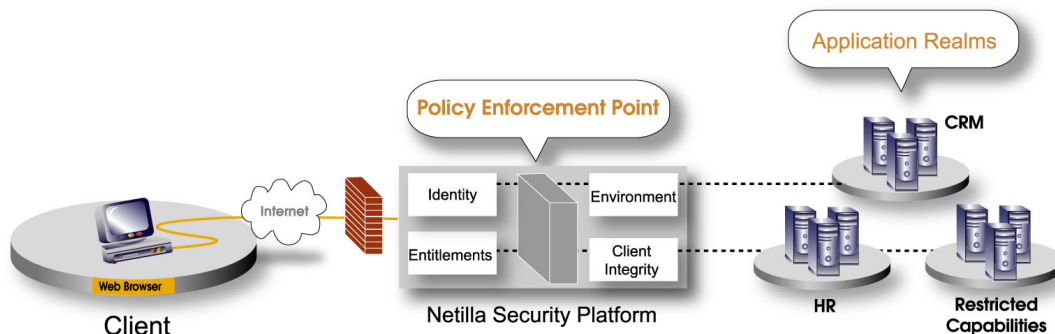
Netilla is currently shipping the following Policy Enforcement Point functionality:

- Dynamic firewall, provisioning session-specific port level access
- Access control by subnet, host/server, or URL fragment
- Host-name hiding
- Up to 10 stages & 1000 unique realms of authentication & policy
- Local/External directory query
- Active Directory/LDAP, Windows Groups
- Broad user authentication types: (Windows, Kerberos, RADIUS, RSA SecurID®, Tokens, Smart Cards).

At the heart of Netilla's policy enforcement engine is the Netilla SecureRealm Framework. SecureRealm combines granular authorization schemes as authentication building blocks, while integrating various policy mechanisms as policy building blocks. These layers are arranged into logical groups, or realms, that represent clusters of authentication and authorization protocols. Each realm can be used to control access on an individual or group-by-group basis.

As shown in **Figure 5**, Netilla's Realm Framework begins by utilizing various authentication schemes (RSA SecurID®, Vasco DigiPass, Kerberos, RADIUS, Windows SMB, LDAP, etc.) as authentication building blocks, while integrating various policy mechanisms (Windows Group, Local Policy, LDAP, etc.) as policy building blocks.

The unique concept is not the number of authentication types, but the fact that they can be logically stacked into a conglomerate scheme for individual users, made up of layers of authentication. A layer represents one of the steps of authentication that the user **MUST** pass



**Figure 4: Application Realms**

before being allowed access to resources on the network.

Bolstering this functionality is the platform's ability to pull policy information at each of the authentication stages, impacting the user's

The result is a flexible and powerful authentication and policy framework that delivers granular control over access to network resources, allowing administrators to group different types of users according to their level of trust or needs, in a manner not easily matched by IPSec or SSL VPN alternatives.

For example, consider a hospital that needs to provide patient information to remotely located physicians. The physician, who is not an employee of the facility, must be given limited access to network resources as a "less-trusted" user. In this case, the physician might be required to pass multiple stages of authentication, such as RADIUS and 2-factor SecurID; be given access only to particular healthcare applications according to an external Windows Group policy server; not be allowed access to external URL's when working within the hospital's intranet, be

denied access to any client/server applications, and be challenged for credentials upon each subsequent attempt to access the hospital network file directory through file sharing.

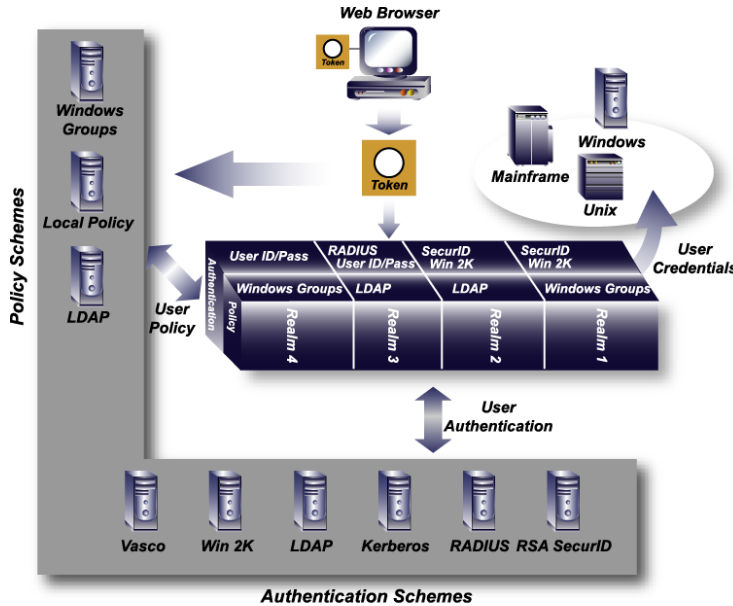


Figure 5: Netilla SecureRealm Framework

capabilities at each stage, refining the user's capabilities once access to resources on the network is allowed. The Netilla platform then takes these building blocks and melds them into an authentication and policy realm.

When a realm member logs in to the Netilla Service Platform, the realm polls its associated authorization and authentication servers, and stores a user profile that is referenced via a Web-based token. This token, acting as a database of authentication and policy, is used to extract the user credentials from the profile that needs to be forwarded to each of the backend servers on behalf of the user. Examples of backend servers include Windows Terminal Servers, UNIX Servers, or mainframes. The policy and authentication determined during the initial logon procedure is therefore active throughout the life of the session, controlling access rights to every access "type" available on the platform (thin-client, client/server over SSL tunneling, and Web applications).

Such a profile, built by integrating various authentication schemes with authorization and policy databases, can be grouped together into a Netilla realm called "physicians," and applied to new users as needed.

In another example, a company's sales manager, who as a member of the private IP network is granted a higher level of trust, would have wholly different access requirements. This user might need to pass only Windows NT authentication; be given access to a suite of applications from multiple application servers according to an external LDAP policy server; be trusted to use local client/server applications such as Outlook, and have his or her credentials continuously presented to the appropriate resource for single sign-on functionality. All of

these authentication and policy variables can be combined into a realm called "Sales."

The result of this synergy is a robust policy and authentication framework that forms the core of the Netilla offering. Multiple external authentication and policy protocols are easily integrated and applied to a variety of users and user groups from a single Netilla platform, which acts as a gateway to network resources as a central point of management.

---

## Market Drivers: Envisioning the Future of Secure Network Access

In order to adequately portray the need to implement policy enforcement when providing access to network-enabled applications, it's useful to sketch a picture of the world we're moving towards, and describe how the use of IP networks are already impacting IT systems.

Contrary to the extravagant claims made during the heady days of the dot com bubble, comprehensive exploitation of the Internet will take time, owing in part to application redesign requirements along with IT operational and resource issues. In addition, the necessary business structures and processes have yet to evolve that will take full advantage of these new information systems. We're only at the beginning of this exciting evolution, but the ultimate future is easy to envision:

1. Eventually, ***all applications will be accessed over the Internet or an IP network*** using standard protocols. The only requirement needed to gain access to an arbitrary application will be an Internet connection and a computer with a standard browser.
2. ***Individuals with an IP-connected PC will employ a diverse range of applications***, and not all will belong to their employer. These programs will encompass "internal" applications and information portals, mission-critical applications used by business systems, service suppliers and partners, as well as applications used to access a vast amount of other information.
3. ***The knowledge workforce will be nomadic, requiring flexible access*** to applications from many locations. This does not

imply the demise of the physical office space; consider that the near ubiquity of business cell phones has yet to threaten the office line. But convenient access to office resources, applications and data whenever a network-connected computer is available will become the norm.

4. ***Authentication will become more complex***; "federated" models of administration and authority will prevail. This means that within a single company, individual departments or business units will define information access roles and responsibilities locally on an individual-by-individual basis, and then between these departments or business units, and then extended to business partners and customers. These delegated structures of authentication and roles can be defined as "security domains". For example, the manufacturing department will create a small number of categories for finance department employees who need access to manufacturing data, and then let the finance department properly assign their employees to those categories. Similarly, enterprises will create a small number of access categories for the employees of business partners, and then delegate the assignment of individuals to those categories to the business partner (and necessarily trust the business partner to adequately authenticate the identify of their employees). Obviously, effective application authentication systems are crucial in these complex and delegated authentication architectures and systems.

5. ***Network security will grow in importance***. As a greater amount of information assets are made accessible throughout the network, the number of protected assets will increase, as will the justification for hackers to attack those assets. Clearly, network security will remain an integral part of application access.

6. ***Reliance on Private Networks will evaporate*** in the face of greater public Internet use. This is a natural consequence driven by the need to provide application access to customers, remote employees, business partners, and remote offices. Use of shared networks (the Internet) is more economical than private networks, simply because capital and operational costs can be amortized across a broad set of users. The less costly Internet

bandwidth (compared to private network bandwidth) is already shrinking private network usage, as service provider networks offer an effective alternative in terms of performance and reliability. The economic motivation to move to service providers will grow stronger as the private network operating costs are amortized on a shrinking portion of the overall network traffic, accelerating the move to Internet use.

7. ***The complexity of network-enabled applications will escalate.*** The earliest Web applications resembled vintage 3270 “green screen” mainframes (where each input led to a new text screen). At that time, even the most basic application access proved vastly preferable to having no access at all, so it made sense to regress to primitive interfaces in order to take advantage of the available Internet connectivity. These early network applications were also limited by slow network performance. By contrast, today’s remote user expects the same rich interactivity they experience with PC-based applications. The sophistication and interactivity of network-accessed applications will continue to evolve in line with the capabilities and cost-efficiencies of the applications themselves.

8. ***Application performance is important.*** 25 years ago, researchers demonstrated that performance was a key contributor to effective computer usage - the better the performance, the better the user’s productivity. With the emergence of the Internet, some of that perspective was temporarily skewed - an application with 40-second response time (unacceptably slow by any existing IT standard) is far better than the hours or days it would take to obtain the same information without the Internet. However, today’s sophisticated user has come to expect the same remote experience that they enjoy in the office, and after all, higher performance still leads to better productivity. Network-accessed applications will grow increasingly sophisticated and interactive as the capabilities of the network improve to support them, and the performance of the applications will be viewed as an important characteristic.

9. In the future, essentially all ***applications will be securely accessed by an increasingly nomadic collection of***

***individuals***, from a diverse set of locations. Access over the Internet will be the norm, as economic considerations shift enterprise network use away from private networks. It will be impossible to define what is “inside” the network and what is “outside”. Fairly quickly, we’ll come to think of everything in the same fabric, with the same set of dynamic degrees of trust and security that are needed inside the corporation replicated when the outside world is involved.

---

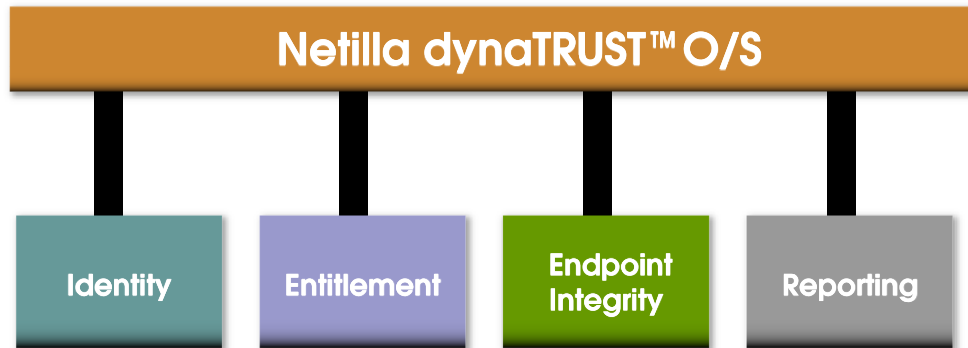
## Providing Secure Application Access Management

In the past, a typical remote access strategy divided “the network” into a simple equation made up of the internal LAN and the external Internet. Essentially, this meant that IT assets were kept within the network, along with most users. The boundary between outside and inside was thus defended in the style of the Maginot Line (the physical fortifications built by France after WWI to defend against attack by the Germans), with the small number of access points open to the Internet well-protected by firewalls and administrative scrutiny. In this model, a user outside the perimeter defenses was the exception, rather than the rule. Internal asset access requirements for those few external users was met by creating a secure data tunnel that brought them inside the network - a virtual private network or VPN.

However, SSL VPNs are changing all assumptions upon which traditional remote access security designs are predicated. The effectiveness of the hardened security perimeter is breaking down as the external user base expands, private networks shrink, and more traffic is channeled through Web-browsing holes in firewalls. In response, rather than providing an external user with wide-open access to all internal assets, the forward-looking goal provides both external and internal users only with access to those assets that they should legitimately use. As Internet use continues to swell and network applications continue to evolve, it is no longer feasible to expect specific security devices to adequately protect everything inside the network. In this new paradigm, security vulnerabilities that threaten internal networks are as significant as those that imperil external systems, simply because threats are no longer limited to external hackers.

This situation requires an entirely new perspective governing application access. There is no longer simply an internal network and an

- Security: Assuring that remote communication is protected from any kind of peeking or tampering
- Network efficiency: Minimizing the



*Figure 6: Netilla dynaTRUST O/S*

outside world. Rather, there are important users everywhere. Information assets must be protected from malicious or inappropriate use from “internal” users as well as external perpetrators. In the near future, we’ll come to think more about securing internal information domains and providing “remote” access to all users based on who they are and what they want to do, as much for “internal” users and “external” remote users. The applications in question will become more bandwidth intensive and performance sensitive over time, requiring careful attention to both network and server optimization. Finally, all of these factors will be operating within a dynamic Internet environment that will continue to be threatened by attempts to steal, deface, and deny access to key information assets. In this environment, remote access solutions must evolve to solve these problems, rather than represent yet another weak spot and vulnerability.

How is this to be done? A remote access subsystem or architecture will need to provide solutions to address or at least participate in the solution of the following problems:

- Authentication: Assuring that the person on the other end is who they claim to be
- Fine grain access control: Using the authenticated identity to provide access only to suitable resources
- Network protection: Assuring that greater external network access doesn’t increase vulnerability to attack, theft or disruption

- network load introduced by remote access to applications
- Server and application efficiency: Minimizing the load that remote access adds to existing applications and servers

### Introducing Netilla dynaTRUST™

Netilla Networks first introduced the Netilla Security Platform (NSP) and SecureRealm Framework in 2001 as a means of enforcing secure remote access with granular, policy-based access control. Recognizing the effect of a broadening nomadic fringe and disappearing network perimeter on enterprise security, Netilla has announced the Netilla dynaTRUST™ Operating System (O/S). Netilla dynaTRUST™ is a policy enforcement operating system for enabling the provisioning of “dynamic trust”. Netilla dynaTRUST™ builds upon the NSP’s policy enforcement architecture to enable the real-time provisioning of “dynamic trust” privileges that are based on the identity, entitlements, and endpoint integrity of the user and/or service.

Netilla dynaTRUST extends the secure remote access policy enforcement capabilities of the NSP, and adds client integrity validation to mitigate potential security vulnerabilities emanating from the nomadic fringe. Netilla dynaTRUST is strategically important because the very use of SSL VPN technology blurs the network perimeter and compromises security. Because all traffic traverses a single firewall port (443), SSL VPN users have “express lane” connections that bypass the perimeter defense mechanisms traditionally used to protect the

enterprise. In so doing, authenticated clients gain access to enterprise resources from a variety of unprotected endpoints outside the scope of control of the organization. Netilla dynaTRUST represents an evolution from conventional static access control, leading to the dynamic provisioning of access privileges that are based on policy rules governing the technical and environmental variables of a user's endpoint.

Netilla dynaTRUST provides a complete, policy enforcement solution that imposes security "best practices" across the nomadic fringe of the network. By ensuring that remote users are in a trusted state before allowing them access to the corporate network, Netilla dynaTRUST:

- Protects cost savings associated with open network-based remote access
- Enables business initiatives such as telecommuting
- Protects productivity gains associated with remote access

Unlike standalone security solutions, Netilla dynaTRUST protects SSL VPNs at every endpoint with policy enforcement services that:

- Employ application-centric firewalls to prevent worms, Trojans, and hackers from gaining access to sensitive corporate data through the SSL VPN tunnel
- Prevent intrusions by analyzing incoming and outgoing communications for malicious behavior
- Check the integrity of SSL VPN endpoints each time users connect to the network, and allow or deny access based on the integrity of the endpoint
- Enforce encrypted access from home networks, hotels and wireless hotspots
- Automatically download and execute missing files, patches, and applications to re-mediate authorized SSL VPN endpoints to a trusted state

Unlike alternative SSL VPN solutions, Netilla dynaTRUST enforces 100% policy compliance, making the remote endpoint a safer place to do business by enforcing policy compliance. Netilla dynaTRUST focuses on four critical security components:

**Identity:** Authentication is the problem of assuring, within reasonable risk, that the individual on the far end of a communication line is who they claim to be. In the past, physical access to a computer or terminal connected to the application, along with a simple password, was an adequate solution. Authorization was granted simply because a user was able to gain access inside the department walls, and could produce a valid ID and password. But a much more robust authentication method is required when access expands to encompass any computer anywhere in the world. The quickly growing reliance of authentication will force the creation of easy to use solutions that also scale effectively. Any effective remote access architecture must integrate effectively with today's authentication solutions.

**Entitlements:** Provisioning role-based entitlement requires fine grain access control. Netilla dynaTRUST addresses this requirement in two distinct ways:

- Deciding what data and function access is appropriate for a specific authenticated individual, and at a given moment
- Enforcing the defined access

Application access systems are a necessary key to unlocking the second item, but they are unable to accomplish this unless access policies are clearly defined and available. In general, this challenge has not been met successfully by current approaches. Of course, in the simpler world before the emergence of network applications, access was typically limited to systems and documents located within a department where physical oversight by managers and colleagues provided much of the necessary control. In today's new situation where anyone can (potentially) gain access to anything from anywhere, the problem of determining suitability is much more complex. It's one thing to "webify" an application and make it easily accessible. The challenge arises from the more complicated need to understand the appropriateness of access, and the granularity requirements that scale individual need with granular access controls. (Of course this assumes proper authentication, careful definition of roles for individuals, and reworking of the application to assure that different access

needs can be supported). Netilla dynaTRUST meets provisions entitlements based on role definitions harvested from leading directory implementations. This enables the enterprise to maintain fluid change management processes when people are hired, fired, change jobs or when the job descriptions or applications themselves transform.

**Client Integrity:** The Internet represents a threatening environment, with no shortage of individuals and groups intent on stealing, defacing, damaging or disabling information systems for both profit and entertainment. The increased productivity brought by remote access should not by itself bring increased risk from Internet-based attack. Successful remote access architecture must respect issues of Internet security. Remote endpoints represent ideal points of attack from the Internet because they are single, externally viewable network resources that possess a large amount of information about internal assets and protection systems. Great care must be taken to assure that no remote endpoint becomes a weak link in the overall security system.

Netilla dynaTRUST's client integrity policy enforcement features can automatically initiate a quarantine action, which can include running a command line, downloading and executing or inserting a file, rechecking the host for compliance, and ultimately granting the now-compliant endpoint with access to the network. This automatic remediation improves the cost efficiency of the system and offers an extra layer of enforcement. Common usages of restoration include:

- Activating a client's anti-virus, firewall, or intrusion detection system (IDS) product if censored show it is not running
- Updating virus definitions, host firewall policies, or host IDS signatures
- Downloading and installing patches, such as to the client O/S or browser
- Changing operating system configurations

---

### The dynaTRUST Alliance Partner Program

In support of dynaTRUST, Netilla has formed the Netilla dynaTRUST Alliance (NdTA), and is collaborating with leading security, identity

management, and client integrity vendors to develop customized policy packages that leverage domain expertise in automated policy enforcement, and consulting expertise developed through working with the world's largest enterprises. With NdTA, Netilla empowers customers with best-of-breed technologies to create a Virtual Trust Domain (VTD), designed specifically to enforce and restore security policies on every endpoint and network access point. VTDs extend protection to every point in the organization, establishing a trust that spans traditional enterprise network boundaries. This trust enables enterprises to continue to deploy productivity-enhancing applications, including Internet connectivity, wireless LANs, remote access, and collaboration applications, while at the same time ensuring that their open networks are compliant to their security policy.

Members of the NdTA Alliance include:

#### **Symantec**

Netilla is collaborating with Symantec to ensure that endpoints are properly protected prior to and during Netilla network access sessions.



Together, Netilla will work with Symantec to deliver Symantec's

next generation client integrity solution, and an API that will allow dynaTRUST to verify the continued presence and status of Symantec's clients during the network access session. If a corporate-issued PC is not running proper endpoint security, the administrator will have the option of defining a policy where full network access will be denied by the NSP. This integration ensures customers of verified end-to-end security during their network access sessions. Integration with a Symantec API will also enable dynaTRUST to communicate with Symantec personal firewall technology to provide the best network protection against new and unknown attack forms.

#### **Benefits of the Solution**

**Proven endpoint security for full network access.** Symantec provides Netilla users that utilize SSL VPN connections with proven endpoint protection against Trojans, viruses, worms and network attacks. Remote PCs remain fully protected and compliant with the corporation's security policy.

**Enforcement:** API integration with Netilla's dynaTRUST™ policy enforcement features verifies that only endpoints protected by Symantec can initiate and maintain network access connections. Insecure endpoints will be refused network access, insuring end-to-end protection of corporate data.

**Central management of security policies:** Netilla provides central management and enforcement of enterprise policies when users connect to the their network via the NSP. Normalizing NSP firewall and policy decision event logs and reporting them into Symantec's Enterprise Security Architecture streamlines the security management burden.

**Technology Leadership:** Symantec's Enterprise Security Manager technology is field-tested and installed in numerous Fortune 500 accounts.

**Supporting the Symantec Virus Prevention engine** and personal firewall as part of client integrity policy enforcement adds an additional layer of anti-virus security. Organizations typically have anti-virus products on corporate PCs and on each application/file server within the network. Netilla dynaTRUST™ will ensure that endpoint anti-virus definitions are always current.

### **WholeSecurity**

WholeSecurity's Confidence Online™ solution provides a clientless, web-based solution for identifying malicious activities introduced by a computer's interaction with public resources.

WholeSecurity's Confidence Online products, like the Netilla NSP, offer clientless deployment and administration, which make these solutions very complementary and cost effective.



WholeSecurity has partnered with Netilla to develop a tightly integrated solution to provide our joint customers with automatic protection against eavesdropping and remote control threats on any computer, anytime. This is a joint development strategic alliance. Netilla and WholeSecurity will collaborate on enhancing their ActiveX agent to perform a variety of client-side security functions, including malware

detection, security patch management, and cache cleansing.

### **Benefits of the Solution**

**Stops Direct Theft and Fraud:** By protecting remote access computers from eavesdropping and remote control threats, Confidence Online reduces online financial and property theft.

**Universal Protection/Compliance:** Confidence Online is so automatic, end users can't undo it. The solution provides universal compliance with company policies and requires only a rapid, one-time user download.

**On-Demand Auditing:** Confidence Online's on-demand scanning capability can ensure that other security solutions like personal firewalls have not been disabled by the user or by malicious programs like Trojan Horses.

**Low Total Cost of Ownership:** Confidence Online's detection and deployment model has significantly lower security management costs than other host-based protection, and it requires no additional Help Desk investment.

**Strong Protection** without affecting user productivity. Like the Netilla NSP, Confidence Online delivers security that won't interfere with users' applications or reduce their productivity gains.

### **Zone Labs**

Zone Labs has partnered with Netilla to ensure that endpoints are properly protected prior to



and during Netilla network access sessions. Netilla will be integrating Zone's Cooperative-Enforcement™ API into dynaTRUST™ to verify the continued presence and status of Zone Labs' clients during the network access session. If a corporate PC is not running proper endpoint security, the administrator will have the option of defining a policy where full network access will be denied by the NSP. This integration ensures customers of verified end-to-end security during their network access sessions. Integration of the Cooperative-Enforcement™ API enables dynaTRUST to communicate with Zone Labs' personal firewall technology to provide the best network protection against new and unknown attack forms.

### **Benefits of the Solution**

**Proven endpoint security for full network access:** Zone Labs provides Netilla users that utilize Network Connect with proven endpoint protection against Trojans, viruses, worms and network attacks. Remote PCs remain fully protected and compliant with the corporation's security policy.

**Enforcement:** Cooperative-Enforcement™ with Netilla's dynaTRUST policy enforcement features verifies that only endpoints protected by Zone Labs can initiate and maintain network access connections. Insecure endpoints will be refused network access, insuring end-to-end protection of corporate data.

**Central management of security policies:** Netilla provides central management and enforcement of enterprise policies when users connect to the their network via the NSP.

**Technology Leadership:** Zone Labs' patented technology, field-tested on over 25 million PCs, automatically blocks new and unknown attacks with its unique "guilty until proven innocent" approach to endpoint security.

### **Sygate Technologies**

Sygate Technologies is a leading provider of security policy enforcement solutions. Sygate's solutions protect corporate and personal networks from intrusion, eliminate the ability of attacks to gain control of corporate information, enforce safe user behavior on all endpoints, and achieve compliance with enterprise security policy. By providing comprehensive security architecture, Sygate maintains a trustworthy computing environment at all times.

Netilla and Sygate will collaborate on enforcing location-based access policies using the Sygate Host Integrity Engine. This engine will provide Netilla with a Win32 client that can be used in lieu of ActiveX to validate that the endpoint adheres to minimum-security standards and that

a personal firewall for the endpoint is operational.

### **Benefits of the Solution**

**Secure access over the Internet:** Netilla provides employees, customers, and partners with secure access to private network resources over the public Internet using a standard web browser. No client software is required; therefore, Netilla's NSP products dramatically reduce the total cost of ownership of a secure access solution.

**Client Integrity:** Sygate provides centrally managed security software for corporate issued PCs. Sygate ensures that remote corporate PCs adhere to the corporate security policy including checking for Trojan horses, the latest anti-virus program, and a PC firewall.

**Protection against hackers:** Sygate also provides a centrally managed ICSA certified PC firewall to ensure corporate PCs are protected against hackers.

### **Microsoft**

Netilla is enhancing its current policy support capabilities, which currently encompass harvesting entitlement privileges from Active Directory, to now include patch and configuration compliance of Microsoft operating systems and applications.



Security experts agree that an overwhelming majority of all security breaches could have been prevented if software patches and updates had been applied when they were first available. In fact, figures from the SANS Institute and the FBI show that the majority of commonly exploited vulnerabilities are due to the failure to apply patches that were available from vendors for several weeks or even a month. However, applying patches is costly and difficult to manage across large enterprises. While applying appropriate security patches in a timely manner is ideal, it is not realistic given resources and limited time, thus providing only partial protection coverage across the network at any given time.

---

## Conclusion

Unlike other SSL VPN products that merely allow remote users to connect to their enterprise networks, the Netilla dynaTRUST O/S offers a policy-based approach that governs access to applications by all authorized users - remote and internal, trusted partner or employee. By simultaneously authenticating users, enforcing policy and ensuring client integrity, Netilla dynaTRUST will speed the evolution from today's static access control to the dynamic provisioning of trust-based access to network resources.

---

### **Copyright ©Netilla Networks, Inc. 2003**

All rights reserved. Use, duplication and disclosure are subject to restrictions.

Netilla Networks, Inc. is the sole proprietor of this document and the material contained herein. This document, or any parts hereof, may not be reprinted or reproduced in any form, by any method, without written permission. For conditions of use and/or reproduction, or permissions to use these materials for publication, contact Netilla Networks, Inc.

Netilla Networks, Inc. reserves the right to revise and improve its products and manuals as it deems necessary. This document provides an accurate description of the product at the time of printing, and may not necessarily be accurate for future releases.

### **Trademarks**

Netilla Networks, Netilla Service Platform, and the Netilla Stylized figure are registered trademarks of Netilla Networks, Inc.