NorthbridgeSecure

Technical Overview 2016/17

2016/17

TECHNICAL OVERVIEW

Contents

Concerned About Network Access?

Need to implement mobility, but worried about security?

NetConnect acts as a gateway between the external world and your internal network and resources. As a single point of control, NetConnect offers you the ability to easily enable mobility for your users without complex changes to your internal infrastructure.

HTML5/SSL

NETCONNECT

Business Applications

Data Center/Physical Server

Active Directory Server

Integration with Active Directory

NetConnect integrates into your local Active Directory environment, so that users retain a single password for all their access points. Upon connecting to NetConnect from their mobile device, users are presented an icon-driven web-top, granting access to the resources they have been afforded permission to access: RDS servers, files, intranet or even their own personal desktop.

Users can connect using a wide range of mobile devices (iOS, Android, PC or Mac) and get the same look and feel regardless of the device they are using, allowing them to switch devices at will, without changing their work practices.

Reporting

NetConnect can track user activity and publish custom user activity reports.

With NetConnect Reporting, it's incredibly simple and easy to produce standard and custom user activity reports (login/logout date and time, applications accessed, source address and more) for auditing, compliance and usage measurement reporting. Not only that, you can arrange reports to be emailed to you at regular intervals.

Track & Report

Key Capabilities

Fine-Grained Access Controls

Control access to URLs, applications and data.

Unified Application Access

Central access to all authorized applications regardless of the server environment (Windows Servers, WEB, Desktop, UNIX and MAC).

Universal Printing

Users can print documents located on Terminal servers to their local printers. No client requirements.

Central Access Solution

External users can use this same internal solution.

Ease of Use

Familiar, icon-driven Web-top delivers a single page for access to various application types.

Easy to Set Up

Web-based administration. Seamless connectivity with authentication and policy servers.

Virtual Appliance Available

Choose from a hardware or virtual solution at no cost.

WITH NETCONNECT SECURITY IS PARAMOUNT.

Security

SSL encryption for secure connections. Strong 2-Factor authentication support (RSA, Securenvoy).

Application Layer Proxy - Applications remain safe on the server and are never directly exposed to public network.

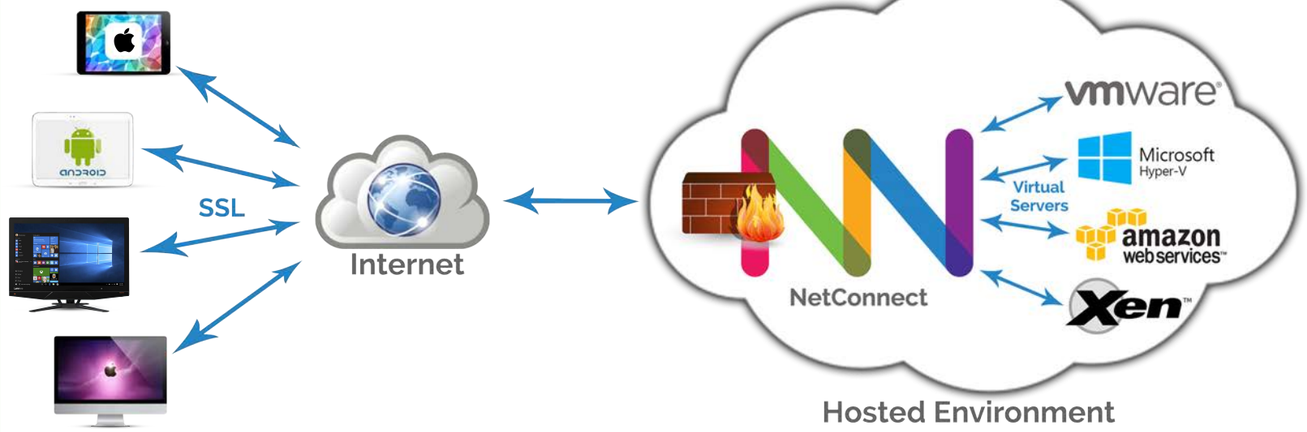
Layered Authentication - Flexible V-Realm framework combines numerous protocols: RSA SecurID®, LDAP, Windows®, NT®, RADIUS, Windows Active Directory, Kerberos, ActivCard (Smart Cards) and more.

FIPS 140-2 Level 4 option.

NetConnect eliminates security risks.

As more companies move toward cloud computing, eliminating security risk is a top priority.

NetConnect Secure Application Access delivers the required security and flexibility in one convenient product. With the availability of virtualization technologies such as VMware's vSphere, companies are now building their own computing clouds. In the client-server computing sytem, the server is a pool of computing resources managed by the company's IT team. These servers can be managed by virtualization technologies such as VMware and tend to be deployed across blade and large enterprise class servers. This can also extend to Cloud providers leading to hybrid solutions or complete migration to a Cloud provider's platform.



Cloud Computing

However, an often neglected part of the cloud is the client side - how do I grant access to applications? And how do I do this securely?

Encrypted communications and strong authentication are just a few of the many measures NetConnect takes to safeguard the network.

How do I transition to Smart Devices (tablets & smartphones etc.)?

Traditionally, cloud clients are desktop computers or "thick clients". Why invest money in optimizing the data centre yet continue to run fat clients? With NetConnect, companies can continue to use their thick clients and plan a phased migration to mobile devices for all users. Additionally, NetConnect's secure and flexible approach delivers a streamlined central, universal access solution to your IT service from wherever you are in the world - anything from a corporate location to an internet cafe!

Issues Created by VPNs.

NetConnect works differently to a VPN. A VPN brings with it a host of issues to the user and organization.

UNSECURE CONNECTION.

A VPN poses a significant security risk to an organization offering full direct access to the network from a device. As such there is very little control over the original device and any malicious software that comes with it.

TIME CONSUMING.

Deploying a VPN can be extremely time consuming as the number of end user devices grow. This is compounded by the growing number of device types available, making the setup and support of VPN very difficult for IT providers.

SECURITY WEAKNESS.

With a large number of devices comes weakened security at every point, and the potential for sensitive corporate data to be lost or stolen. With a VPN, the device can retain sensitive information, and if lost or stolen can place the organization at risk.

Issues Resolved by NetConnect.

NetConnect works differently to a VPN. NetConnect only allows specific traffics between the user device and the target resource. This allows NetConnect to further secure Remote Desktop connections and file access.

DATA IS SAFE.

NetConnect strengthens a basic RDP connection and file access by only allowing the RDP application, or app on mobile devices, to communicate with the server. The remote device is only 'seeing' the application, so no data ever leaves the organization.

SETUP IS EASY.

NetConnect is deployed through one clientless point of access for PC and Mac* allowing users to be enrolled in minutes while significantly reducing involvement from internal IT.

BYOD READY.

NetConnect reduces complexity of roll-out through clientless point of access, with a specific secure app or web browser for any device.

* Browser Only

The NetConnect Security Difference.

Username & Password

NetConnect integrates to your Active Directory, allowing you to control the user identity as they would in the office.

Secure Communication

All communication is fully SSL encrypted at the highest possible level.

2 - Factor Authentication

NetConnect natively integrates with multiple 2FA solutions, including RSA and SecurEnvoy, making your connection even more secure.

Reduced Network Communication

NetConnect only allows targeted communication to take place between the correct application on the mobile device and the target resource on your network, ensuring the security of the end user's device is never a problem.

NetConnect Operates Exclusively on Port 443

Allowing you to operate without uneccessary open ports on your firewall.

Leaves No Footprint

NetConnect enables users to work on their data and connect to your servers. No data is ever left on the device, removing the risk of data leakage in case of theft or loss of a device.

NetConnect Feature Set

FEATURES	EXPERIENCE WITH VPN + RDP	EXPERIENCE WITH NETCONNECT
CONNECTING TO THE NETWORK	• Each user needs to be set up individually, and the setup required is different for all device types (i.e. Android, iOS, PC, Mac). If users aren't IT savvy, setting a VPN or RDP up for themselves can be difficult. • Passwords are usually stored on the device, compromising security and access if the device is lost.	• Users download an app or browse to a single URL, enter their username and password - and the connection is working. • Passwords are not stored on the device or the NetConnect environment but only the Active Directory so that data loss is not a risk.
NETWORK SECURITY	• Upon connecting to a VPN, a user's entire device is connected to the network. This opens the organization's network to any virus present on the user device, creating an unneccessary risk.	• NetConnect only allows a RDP session to be active, which cannot be leveraged by viruses. The device is not fully connected to the network, and so the network remains secure.
ACCESS TO COMPANY FILES	• Data is synchronized and exists on the user device, presenting a security risk or data breach should the device be lost or stolen, or if staff leave the organization. • As a result, BYOD is difficult to implement and requires additional expenditure such as MDM to address permission issues.	• Data remains in the office or on the server - data is **never lost.** • Implementing BYOD is simple. Devices are only providing a window into the application, meaning **no data ever leaves the organization.**
USER DEVICES	• A standard issued laptop or smartphone carried between the office and home retains a wealth of sensitive company data.	• Users connect seamlessly from any device and can travel with only a tablet or smartphone. This becomes particularly appealing to any corporate traveller from Sales to 'C' level employees.

NetConnect removes the complexity of deploying a VPN by providing a clientless point of access for PC & Mac*, in addition to a specific secure app for iPad, iPhone and Android, securing the communication between device and environment further.

*Browser only.

NetConnect Feature Set

FEATURES	EXPERIENCE WITH VPN + RDP	EXPERIENCE WITH NETCONNECT
CONNECTING TO 'MY' DESKTOP	• User selects a free RDP client and sets up their Desktop IP address, which is likely to change environment through the use of DHCP. This often requires internal IT support and is often unreliable, posing significant security risks.	• By using the NetConnect client, a user's desktop is always accessible even if the IP address has changed. Connectivity is reliable and highly secure.
WORKING ON MULTIPLE SERVERS	• Users need to set up **multiple RDP Sessions manually.**	• RDP Sessions are defined in one central location, on the NetConnect server.
MANAGEMENT	• IT administrators must regularly patch the VPN, usually due to **security concerns.** • Cutting off user access is time consuming.	• Cutting off user access is a **single click.** • The NetConnect server is built as a secure platform from the ground up, and **does not need to be patched as regularly.** • NetConnect is focused solely on managing remote access, prioritizing the potential of attack and making it less susceptible.
CONNECTING FROM HOTELS & CAFES	• VPN's can often be blocked from public places, rendering them **mostly useless.**	• NetConnect only uses **Port 443**, making connection possible from anywhere, through any standard firewall, at any time.

NetConnect removes the complexity of deploying a VPN by providing a clientless point of access for PC & Mac*, in addition to a specific secure app for iPad, iPhone and Android, securing the communication between device and environment further.

*Browser only.

CONTACT US:

SALES ~ sales@northbridgesecure.com

ONLINE ~ northbridgesecure.com

PHONE ~ +612 8424 7900

ADDRESS ~ 50 Broughton Rd, Artarmon NSW 2064 Australia