Deploying NetScreen Remote Access Solutions

March 2002

A White Paper By
NetScreen Technologies Inc.
http://www.netscreen.com
**Table of Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Choosing a VPN Technology</td>
<td>3</td>
</tr>
<tr>
<td>Authenticating Remote Users</td>
<td>8</td>
</tr>
<tr>
<td>Deploying NetScreen-Remote Software</td>
<td>14</td>
</tr>
<tr>
<td>Summary</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction

Internet-based VPN that provide mobile-workers with remote access can lead to substantial cost savings over legacy RAS technology. The NetScreen Whitepaper “Solving Business Problems with Virtual Private Networks” describes in detail the cost savings and business challenges that VPNs provide and solve. VPNs have become the new standard for enabling remote access for mobile workers, remote offices and business partners. As administrators have learned from initial deployments or evaluations of some VPN products, VPNs can add additional complexity for end-users, requiring training and education of users and handling more support calls. Choosing a VPN technology, integrating an authentication solution and deploying VPN client software have traditionally been roadblocks an Administrator will face when deploying remote access. The NetScreen remote access solution addresses a number of deployment and management problems that have traditionally been barriers to implementing VPN-based remote access.

NetScreen provides a complete remote access solution that will scale to the needs of any organization through our high-speed NetScreen devices, Global PRO line of security management systems and NetScreen-Remote client software. This paper will focus on planning and deployment of remote access solutions using NetScreen products, it will also discuss integration with existing user authentication, X.509 certificate and NetBIOS networking technologies that are necessary in large deployments. This paper is targeted to the technical network or security administrator who is evaluating remote access solutions or planning a deployment with NetScreen products. It is assumed that the reader is familiar with the basic concepts of encryption, TCP/IP and Windows networking.

Choosing a VPN Technology

IPSec and IPSec/L2TP are two industry-standard remote access VPN technologies that are supported in all NetScreen products. Each technology has its benefits, drawbacks and ideal use-cases. Each provides for tunneling, authentication and encryption of traffic making them suitable protocols for remote access. The following section will first look at IPSec and then L2TP VPN technologies.

IPSec is a combination of transport security protocols and key-exchange protocols designed to work in tandem to provide secure authentication, encryption and tunneling of IP Packets across any IP network, such as the Internet. encryption and authentication are provided via the use of Encapsulating Security Payload (ESP) or Authentication Header (AH) protocols. You may often hear a VPN connection referred to as an IPSec tunnel, in this case ESP is being used in tunnel mode to encrypt IP Packets during transit. Tunnel mode refers to the concept of wrapping a second IP header around the original IP packets, and they are therefore “tunneled” inside an encrypted ESP packet. This leaves the original IP packet untouched, including the original IP header fields like source, destination address and data payloads. The original IP packet remains completely encrypted within the ESP Packet (Figure 2-1.) Since the packet’s original IP Header remains untouched Private IP Addresses can be tunneled through the Public Internet remaining hidden from view. If someone were to intercept the IPSec packet, they would not find any identifying information in the encrypted packet, not even original source and destination addresses.
IPSec AH provides only for authentication of packets (no encryption) and is rarely used today. ESP provides for both encryption and authentication and is the most commonly-used IPSec protocol. All NetScreen Devices support both ESP and AH. Both protocols use cryptographic keys to provide for encryption and authentication of packets. NetScreen products support common encryption algorithms including DES, 3DES, AES128 and AES256 and authentication algorithms including MD5, SHA-2, SHA-256.

The Internet Key Exchange Protocol (IKE) - while not required by IPSec, is necessary in any sizable deployment. IKE enables two IPSec systems to negotiate a Security Association (SA.) An SA defines a set of algorithms and keys to use for an IPSec Tunnel. Each IPSec host or gateway communicating will send Identity information about itself to the peer. NetScreen products match an IP Address, Email address, Fully-Qualified Domain Name (FQDN) or an X.509 certificates Distinguished Name (DN) to verify a remote peers identity. Each IKE identity corresponds to a specific VPN access policy, pre-shared key or certificate and other parameters required to negotiate an SA. One benefit to NetScreen’s integrated firewall and VPN functionality is the ability to match VPN User identities to specific firewall policies, which can include limiting access to specific hosts, subnets or services in addition to scheduling, traffic shaping and other firewall capabilities. These policies also become the basis for IKE Phase II.

During Phase II of IKE NetScreen products will create the security association based on VPN policies and security parameters defined in the device. If multiple policies are tied to a specific identity, an equal number of SAs will be negotiated. Once the IPSec Tunnel is active, only valid traffic matching the policy will be sent across this tunnel – unauthorized traffic will be blocked. Access may be limited to a specific host or subnet behind any interface of a NetScreen device.

During IKE NAT-discovery is also performed. Since IPSec does not work well in a NAT-environment, a message exchange detects the presence of NAT between the IPSec hosts. If NAT has been detected NetScreen devices will enable NAT-Traversal for that connection. NAT-Traversal allows IPSec traffic to traverse through NAT, which has traditionally been problematic. This is because NAT has modified the IP headers of packets causing IPSec authentication checking to fail. NAT-Traversal encapsulates the entire ESP packet inside UDP for transmission through a NAT device, the UDP packet can be modified by the NAT, leaving the original IPSec packet inside unmodified during transit (Figure 2-2.) ScreenOS 3.0 and NetScreen-Remote 7.0 support this industry-standard method of NAT-Traversal. NAT-Traversal is automatic and no user-configuration is necessary. Users will always be able to establish VPNs from anywhere without any reconfiguration. NetScreen’s standards-based UDP NAT-Traversal uses less overhead than other TCP based solutions ensuring quicker tunnel setup times and faster throughput.

<table>
<thead>
<tr>
<th>IP Header</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical TCP/IP Packet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Header</th>
<th>ESP Header</th>
<th>Orig-IP Hdr</th>
<th>TCP</th>
<th>Data</th>
<th>ESP Trailer</th>
<th>ESP Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Same packet encrypted with IPSec Tunnel

Figure 2-1: IPSec ESP Packet

Typical TCP/IP Packet and same packet encrypted in IPSec Tunnel. Notice original packet is stored encrypted inside ESP Packet.
Deploying NetScreen Remote Access Solutions

The combination of integrated tunneling, encryption and authentication makes IPSec an ideal protocol suite for remote access. IPSec has been an industry standard for 10 years and interoperability is strong. NetScreen Products are compatible with all RFC-Standard IPSec implementations. The IPSec Protocol itself does have its limitations; it only protects IP unicast traffic, it was not designed to transport broadcast and multicast traffic and cannot protect Non-IP traffic.

<table>
<thead>
<tr>
<th>IPSec Protocol</th>
<th>Usage</th>
<th>Description</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP</td>
<td>Encryption &amp; Authentication</td>
<td>Provides for Encryption and Authentication of IP Packets</td>
<td>IP 50</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Only</td>
<td>Provides for only authentication of IP Packets</td>
<td>IP 51</td>
</tr>
<tr>
<td>IKE: Phase I</td>
<td>Key Exchange</td>
<td>Negotiates Security Association (SA)</td>
<td>UDP/500</td>
</tr>
<tr>
<td>NAT-Traversal</td>
<td>Identity Checking</td>
<td>IKE Identities are exchanged &amp; authenticated</td>
<td></td>
</tr>
<tr>
<td>NAT Discovery</td>
<td></td>
<td>Discovery of NAT-Device between connections</td>
<td></td>
</tr>
<tr>
<td>XAUTH (Optional)</td>
<td>Extended Authentication</td>
<td>Provides Pre-IKE User-Based Authentication &amp; IP Assignment.</td>
<td></td>
</tr>
<tr>
<td>Phase II</td>
<td>Policy Checking</td>
<td>NetScreens negotiate hosts, subnet or range of addresses to access, policy checking is performed.</td>
<td></td>
</tr>
<tr>
<td>Proxy ID</td>
<td>IP Policy Checking</td>
<td>NetScreens negotiate use of ESP, or AH, Tunnel or Transport mode and which cipher and hash algorithm to use for each connection (AES, 3DES, DES, MD5, SHA-1, etc.).</td>
<td></td>
</tr>
<tr>
<td>SA Proposal</td>
<td>Negotiate Security Association</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Layer 2 Tunneling Protocol (L2TP) is another industry standard method for tunneling and authentication designed to replace PPTP, a legacy tunneling protocol. L2TP is a tunneling protocol, which requires user authentication and provides remote client IP addressing based on user identity as an extension to PPP. Since the native-encryption used in L2TP is inherently weak it should be used in conjunction with IPSec for good security (Figure 2-5.) IPSec provides for encryption and machine-based authentication while the L2TP, encrypted by IPSec provides for user-level password authentication and IP Assignment (Figure 2-4.) This is known as IPSec/L2TP and is quickly becoming the RAS VPN standard for those who wish to integrate password authentication with remote access on Windows platforms. Native support for L2TP/IPSec is present in Windows 2000 and above and NetScreen-Remote supports IPSec/L2TP on Windows 95 and newer platforms.
When using L2TP with NetScreen devices, users and IP pools defined in the NetScreen device, or on an external RADIUS, a SecureID or LDAP server may be used to authenticate users. Administrators may also query for a user’s IP pool information directly from RADIUS, allowing users to be assigned a specific address each time they connect, as defined in the RADIUS Server. NetScreen also implements RADIUS accounting, allowing for the RADIUS server to know when users have connected and disconnected, as well as which IP address was assigned, making integration with an existing AAA system easy. In many environments where Dial-Up POP systems are in use, a RADIUS server already exists with IP pool information. With this functionality migration from Dial-Up POP systems using RADIUS to a NetScreen remote access VPN is possible without re-entry of users or network re-addressing. A remote user’s DNS and WINS servers may also be assigned, enabling users to browse the internal corporate network using the same hostnames they are familiar with inside the corporate network.

L2TP is encapsulated inside IPSec to provide for node-node encryption & authentication of packets
L2TP protected by IPSec provides tunneling, user-authentication and IP Address for Remote users
L2TP tunneling is provided by use of a Virtual Interface on the NetScreen-Remote users PC
NetScreen-Device can verify L2TP Username & Password against external RADIUS Server

Figure 2-5: Use of L2TP over IPSec
L2TP protected by IPSec provides user authentication and IP Assignment to NetScreen-Remote users and IPSec provides for encryption of L2TP Packets.
The L2TP protocol itself does have some limitations, for one it can only be used on Microsoft Windows platforms. Additionally it adds approximately 15% overhead to traffic causing slight performance degradation compared with traditional IPSec only VPNs.

Regardless of the VPN technology chosen, NetScreen products implement a number of unique features that extend beyond standard VPN protocols. These features include policy-based management, NetScreen Redundancy Protocol (NSRP) high-availability and Hub & Spoke topology support.

All NetScreen Products permit VPN access based on policies, this is known as policy-based VPN. A policy can be in the form of a standard firewall policy, or a specific VPN policy. Large numbers of policies may be defined to give specific access to outside hosts, specific remote users or groups of users. NAT can be performed on a per-policy basis, changing the source or destination address of packets prior to encryption or after decryption. Traffic shaping rules can be applied to every policy, enabling guaranteed bandwidth levels for specific applications or remote users. Additionally authentication parameters, scheduling and accounting are all defined on a per-policy basis, giving administrators ultimate flexibility.

NetScreen-Global PRO and Global PRO Express include the NetScreen Policy Manager, a unique tool that allows policies to be defined on a global basis, and applied to devices or users easily. Policy Manager moves the management of security away from the model of managing policies on individual devices into a global model where policies are centrally defined and applied to devices and users. These “template” policies greatly reduce the total configuration required by the administrator when a large number of polices are required. Policy Manager also includes the VPN Wizard, enabling the creation of both meshed and Hub and Spoke VPNs in an easy-to-understand point-and-click manor. Policy Manager takes care of creating each connection necessary, defining all VPN attributes and configuring NetScreen Devices as necessary. A detailed description of NetScreen’s policy management architecture can be found in the whitepaper entitled “NetScreen’s Approach to Policy-Based Management”. Policy Manager also facilitates the secure distribution of VPN Policies to NetScreen-Remote Users. This is explained in more depth in section 4.

NetScreen Redundancy Protocol (NSRP) enables both active-passive and active-active high-availability (HA) models. NetScreen devices that support NSRP are able to fail over in sub-second times while retaining VPN Sessions & Users – This is known as stateful failover and is critical in sizable remote access deployments. If a central NetScreen device were to fail, for mechanical or network reasons, the HA peer would become active immediately, and continue to serve all active sessions for both Remote user and Site-to-Site VPNs. Maintaining sessions during failover is critical with Remote Access, as it enables users to continue working in their applications without noticing any network interruptions and only a short sub-second delay in application response. For more information on NSRP please see the whitepaper entitled “High Availability Solutions & Technology for NetScreen’s Security Systems.”

Traditionally VPNs have operated on a fully meshed model where remote users connect to gateways directly for access to the network protected by that device. With 10 site-offices there could be up to 10 tunnels established. The advantages of the fully meshed model are lower-latency and each office having direct control of remote users. Hub & Spoke allows remote users to connect to a single NetScreen device (Hub), that device in turn connects to other NetScreen devices (Spokes) via site-to-site VPN. In this model the central hub has complete control over remote user access rights. Users need only be added to the central site to gain access. This also requires the remote user establish only single tunnel directly to the hub to gain access to multiple remote networks. Multiple hub’s may exist each with their own spokes in a large network. If the hub’s are connected together connectivity extends to each of the spokes. NetScreen’s unique implementation of policy-based VPNs gives the administrator great flexibility when designing the network or migrating existing networks to NetScreen products.

IPSec and L2TP/IPSec are both secure, reliable technologies well suited for deploying remote access. NetScreen’s implementation of these technologies on its entire product line, with
Deploying NetScreen Remote Access Solutions

hardware acceleration enable Enterprises and Service Providers to deploy large-scale remote access VPN services to users with fast, reliable connectivity. Unique NetScreen VPN features such as policy-based management, NSRP and Hub & Spoke give the administrator the power and flexibility to deploy mission-critical remote access with ease. VPN encryption with AES or 3DES encryption make it impossible for eavesdroppers to intercept or view remote users traffic. However, the weakest link in a remote access VPN can be the authentication of remote users. The technology chosen to authenticate remote users is often a balance of usability and security.

**Authenticating Remote Users**

Choosing a technology to authenticate remote users will likely be the most involved and important decision when implementing a Remote Access VPN. With the myriad of technologies available this decision can be quite involved. Will the authentication system integrate with your existing user-database? When migrating or using an existing database of usernames and passwords the answer to this question prior to making a decision on a technology is very important. Will it be easy for users to understand and use on a daily basis? Consider the computer skill level of your users. If users must install drivers or perform additional complex tasks it may generate a large amount of support calls during the initial deployment and also day-to-day maintenance of the system.

A good authentication system will require a user to present something they have (e.g., a key, token, smart-card, fingerprint or random number) with something they know (e.g., a password.) This is known as "two-factor" authentication. Unfortunately most legacy authentication systems operate on a username and password model, requiring only that the user know something (their password) in order to gain access. While this is easily understandable for most users it is not the most secure. A compromised password means anyone could gain access to critical information. While the risk may not be considered too great for PCs secured on a company's premises, it becomes an open back door on a remote access device. Fortunately today's VPNS provide the ability to choose from multiple authentication technologies for compounded security.

NetScreen products support a wide-range of user-authentication options for remote access users. SecureID and Smart-Cards allow for two-factor authentication of the user. Smart-Cards are gaining popularity as a method for authenticating users within the native compatibility of IPSec using certificates. Smart-Cards using X.509 certificates provide for unique user-identification during IKE and also use two-factor authentication. Additionally Smart-Card technology has become standards-based and native support is available in most Windows platforms.

Certificates and Preshared keys are used natively in IPSec/IKE for machine-based authentication. During the first key exchange messages, The NetScreen VPN Gateway will authenticate each remote-machine by matching an IKE Identity with a valid certificate or preshared key. The certificate and preshared key then become seed material for the encryption scheme used for that session. With NetScreen-Remote this does not require any user-intervention, the preshared key and certificate are selected in the policy file and loaded into the program on the machine - "something you HAVE". When a user attempts to access a protected network resource, the IKE key exchange and authentication occurs transparently to the user. This works well for machine-based authentication, as a user need not be physically present to enter a password. This is the model with which site-site VPNS operate, and security remains extremely strong provided the VPN gateways themselves are not compromised, which is virtually impossible with NetScreen devices with proper access controls configured; However, when VPNS are used by remote users on general purpose PCs with limited access control, machine-based authentication alone will not suffice. Consider if a laptop or hard-drive were to be stolen - anyone who recovered the machine could potentially gain access to the VPN!

Certificates can also be used for user-authentication, provided the remote users private key is kept secure. PKI operates on a trust model, when a users key is approved or signed by the Certificate Authority’s (CA) private key, the CA Administrator is saying "I trust this user." The user themselves will also say "I trust this CA" by loading the public key of the CA itself and trusting.
certificates that have been signed by that CA (Figure 3-1.) When NetScreen devices are configured to trust a CA, they have an implied-trust of all certificates that have been signed by that CA, such as certificates for remote users. Compare the certificate trust model to a driver’s license. The personal information on a driver’s license must be validated prior to having the seal of approval imprinted by the DMV. Thus someone can prove whom they are and that they are a valid driver by presenting a driver’s license.

NetScreen devices look at a certificate’s distinguished name (DN) to obtain identity information. All certificates contain a DN that uniquely identifies it with a serial number, date, and user information such as name, organization, organization unit, city, country or email address. The NetScreen Device can pick any part of the DN to identify users and match them to specific VPN Policies. When defining a Certificate-based VPN for all users whose Organization is NetScreen and Organizational Unit is Sales ”O=NetScreen;OU=Sales” would be defined when adding a remote user VPN to the NetScreen-device. The NetScreen will permit multiple users to login provided their certificate contains this identity information and has been signed by the trusted CA. This enables granular remote access policies to be defined for a group of users while only requiring the Administrator to configure Group-Identity information in the NetScreen device. This eliminates the need to add each remote user to the NetScreen Device, instead a Group-Identity is created for a subset of users, and users are added and removed through the CA Infrastructure, by signing or revoking certificates. This feature is known as Group-IKE ID and is available in ScreenOS 3.0 and above.

Smart-Cards are becoming an increasingly popular method of uniquely identifying users with certificates. They have been used for quite some time in high-security environments, such as government, financial and aerospace corporations. A Smart-Card stores a user’s identity information and encrypts it with a password that only the user knows. When a user wishes to
authenticate with the Smart-Card they must place their card in the reader device, and enter the password for their card - much like an ATM card. This provides good two-factor authentication as the user must have their Smart-Card and know their password. The password is then used to decrypt the encrypted private key on the card into RAM on the Users PC for use with an application (Figure 3-2.) The NetScreen-Remote client will then use the private-key to sign initial key-exchange during an IPSec/IKE session.

**Figure 3-2: Smart-Card Trust Model**

A Smart-Card enables a user to store their Private Key on a removable card, to establish a connection the user must insert their Smart-Card and enter the password to unlock the private key stored on the card. This provides two-factor authentication with Certificates.

Deployment of certificates to large-number of remote users machines has traditionally been a barrier for using PKI with remote access; However, Smart-Cards have made the deployment of large numbers of certificates much easier. The administrator can configure Smart-Cards on behalf of a remote user and simply hand the card and initial password to the user. Once the user receives their card they simply change the password and keep their card safe. If a users access needs to be revoked, the Administrator simply revokes the users certificate in the PKI system. The NetScreen device will deny access if a revoked user attempts to connect by checking the Certificate Revocation List or directly via Online Certificate Status Protocol (OCSP.) Going back to the DMV analogy, this would be similar to a police officer running a license through the database to ensure it is still valid.

NetScreen products simplify the deployment and ongoing management of certificates for remote users and NetScreen gateways. NetScreen-Remote 7 provides the capability to bundle both a CA Certificate and User Certificate with the software installation. So even without using Smart-Cards certificate deployment can be seamless. Integration with Microsoft Crypto API (MSCAPI) allows users to simply double-click to load certificates into NetScreen-Remote, as well as native support for MSCAPI compliant Smart-Cards. Additionally, users can use existing certificates loaded in their web-browsers or other MSCAPI applications for VPN authentication. These
features greatly simplify the deployment of certificates to a large-amount of end-users, as is the case with remote access.

NetScreen devices can automatically submit certificate requests to receive their certificates and CA certificates from CAs supporting the Simple Certificate Enrolment Protocol (SCEP) including VeriSign, Entrust and Microsoft CA’s. When a certificate expires, the NetScreen device will automatically submit a new request and download new certificate when available. SCEP eliminates the need for the administrator to manually create and submit certificate requests for each device, which has traditionally been a painful process for anyone with a large number of devices.

Certificates are not for everyone, some administrators may wish to use their existing user database. In most large enterprises and services providers this will likely be a central user database shared by many applications, such as a RADIUS, SecureID, LDAP or NT Domain. These authentication systems are often in-use by environments that have consolidated all of the multiple authentication systems into one. These systems allow administrators to store and manage users passwords in single database while allowing applications and network devices to leverage that database for authentication. This is often done to simplify the management of large numbers of users, eliminating the need to update and manage passwords in multiple systems. The NetScreen line of integrated security systems allows remote access VPN users to authenticate against existing RADIUS, SecureID or LDAP (Active Directory) databases. NetScreen devices provide for up to 3 backup authentication servers for redundancy. If the primary contact fails the NetScreen device will attempt to contact alternative servers to authenticate the user.

Integration with virtually any third-party database can be achieved by use of a RADIUS-Proxy. Most RADIUS Servers including Microsoft and Funk support the proxy of authentication request to off-board databases, such as SQL, NT Domain, Novel, NIS Domain and others. Since NetScreen Devices support RADIUS, virtually any authentication systems can be used through a RADIUS Proxy.

Since this type of user authentication is usually password based, with the exception of SecureID, it is highly recommended to combine this authentication with IPSec preshared key or certificates to provide for machine-based authentication. Requiring users to know something (their password) and have something (their certificate, Smart-Card or PC itself) in order to gain access to the VPN, leads to a more secure, controllable remote access solution.

**Authenticate & Go**

With NetScreen Global PRO, NetScreen-Remote users can authenticate to the Global PRO system prior to the secure download of a VPN Policy to that machine. When a user wishes to login to the Remote Access VPN, they launch the NetScreen-Remote Login program and enter their username and password. The NetScreen-Global PRO system will authenticate the user against its existing LDAP database or can also query an external RADIUS database if necessary (Global PRO 3.1, Target Availability Q2/CY02). Since the Remote User is authenticated prior to the retrieval of VPN configuration and keys, overall security of the remote access system is improved. All VPN configuration information is purged from the NetScreen-Remote User’s machine upon logout, eliminating the possibility of a stolen laptop being used to gain unauthorized access to the network. This enables a more controllable remote access solution. NetScreen’s unique approach to authenticating remote users prior to VPN policy retrieval allows the Administrator to deploy standard-IPSec with password authentication. For information on configuring VPNs in Global PRO and applying them to devices and users, please see the NetScreen-Global PRO Administrator Guide.

Other methods of user authentication can be used with or without NetScreen-Global PRO include L2TP and IPSec Extended Authentication (XAUTH). Both differ from NetScreen-Global PRO, which authenticates users prior to VPN policy download. L2TP and XAUTH provide authentication during VPN tunnel setup with the capability to integrate into a RADIUS, SecureID.
or LDAP Database. With L2TP and XAUTH the user is prompted for login credentials automatically each time the VPN is established, whereas with Global PRO users must initiate the login process and enter their credentials prior to accessing VPN resources.

L2TP, described in Chapter 2 provides user-based authentication through the PAP/CHAP Protocols. NetScreen Devices can query client L2TP information directly from RADIUS, SecureID or LDAP Servers. IP Pools, described later in this section may be locally defined in the NetScreen or queried from an external RADIUS Server and applied to specific users or groups. Internal DNS and WINS addresses may also be assigned to clients, enabling seamless access to internal hosts and the Microsoft network neighborhood. Since native support for L2TP is present in Windows 98 and above, the necessary software for L2TP will likely be already installed on most machines.

XAUTH is an alternative to L2TP, which provides for user-based authentication during IKE. XAUTH provides the same legacy-authentication and IP Address support as L2TP, without the additional overhead. XAUTH is not an IETF Standard Protocol; however many vendors including NetScreen choose to implement it. When using NetScreen-Remote with XAUTH enabled, a password prompt will be displayed to the user each time a VPN is initiated, the password submitted may be matched against a user defined in the NetScreen Device, or an external database. IP Pools are also created in the NetScreen or queried from external RADIUS. IP Pools may be locally defined in the NetScreen or queried from an external RADIUS server and applied to specific users or groups. DNS and WINS addresses may also be assigned to clients with XAUTH (Figure 3-3.)

IP Pools used with L2TP and XAUTH provide for granular access control of remote users through any IP network. NetScreen-Remote users traffic will contain the IP Address assigned from the pool whenever they send traffic through the VPN, as opposed to using their public assigned IP Address. Since IP Pools may be applied to user-group or individual users as they authenticate, other devices in the network will be able to filter remote access based on these IP Pools. If an administrator wanted to restrict sales IP Pool (172.16.5.0/24) from accessing engineering subnet, protected by the engineering router I could simply block traffic from 172.16.5.0 from entering the engineering LAN. This gives the administrator the flexibility to restrict VPN access inside the network based on the IP Address of the remote user.
NetScreen-Devices may query IP Pool information from RADIUS servers. This allows specific IP addresses to be assigned to remote users based on username or group membership information stored on the RADIUS Server.

Administrators may wish to leverage an existing NT Domain or Active Directory user database for authentication of remote users. The NetScreen provides the ability to query an existing Active Directory (LDAP) allowing users to keep the same passwords as their domain login for simplicity. NT 4.0 Domain integration can be achieved via the use of a RADIUS-Proxy or installation of the Microsoft ISA RADIUS Server. Since the users passwords are stored in a single location, administration of users and password synchronization are performed on the NT Domain itself, making ongoing management of users straightforward.

NetBIOS resources may be accessed transparently over a VPN. NetScreen-Remote users may be members of an NT Domain and authenticate to the domain when accessing network shares or the Microsoft network neighborhood. To use this functionality NetScreen-Remote clients must have one valid WINS Server defined in their TCP/IP Configuration. If L2TP or XAUTH is used these addresses can be automatically assigned to the client when they login. Users who are logged in will be able to view other active machines in the Network Neighborhood as well. If accessing a Workgroup without NT Domain or WINS, L2TP must be used, as it provides transport of NetBIOS broadcast messages across the VPN, required by Microsoft networking. Since broadcast messages can consume a lot of network bandwidth this is only practical in smaller deployments with a few remote users.
### Authentication System | VPN Protocol | Manual Key | Preshared | Certs | IP Pool Source
--- | --- | --- | --- | --- | ---
NetScreen Internal User Database | IPSec or L2TP | Yes | Yes | Yes | Internal
RADIUS | IPSec with XAUTH or L2TP | L2TP Only | Yes | Yes | Internal
SecureID | IPSec with XAUTH or L2TP | L2TP Only | Yes | Yes | Internal
LDAP | IPSec with XAUTH or L2TP | L2TP Only | Yes | Yes | Internal
Active Directory | IPSec with XAUTH or L2TP | L2TP Only | Yes | Yes | Internal
NT Domain w/ ISA Server | IPSec with XAUTH or L2TP | L2TP Only | Yes | Yes | Internal

**Figure 3-4: Overview of authentication supported in NetScreen Products**

The decision of which authentication system to use for remote access will depend on existing systems, the level of security desired and computing skills of the end-users. NetScreen Products integrate with most authentication systems directly or through RADIUS-Proxies giving the Administrator the ability to integrate with existing systems already in-use. An administrator should choose a system that scales to the needs of your users and network, meets the security requirements and is straightforward for the end-users to use. The choice of authentication should be carefully evaluated and planned prior to deploying NetScreen-Remote client software or any remote users.

### Deploying NetScreen-Remote Software

Once VPN technology and authentication system have been selected, planning the deployment of NetScreen-Remote client software can begin. NetScreen-Remote 7 contains a number of new features that ease large-scale installation of the software, eliminating the need for users to enter configuration or installation information ensuring that the correct configuration is always installed. In any sizable deployment it is recommended that the Administrator repackage the software and create a custom installation for end-users.

Creating a custom installation requires modifying a configuration file in the install directory of the NetScreen-Remote software. This file, OEMSETUP.INI allows the Administrator to define parameters for installation of NetScreen-Remote software including: Program Group for default installation, Default path for installation, which components to install, shortcuts to install and automatic Reboot after installation. This file allows the administrator to lock down the installation parameters and/or hide the program itself from the user. With this it is possible to create an installation that will run without user-intervention, automatically reboot the machine and install default VPN policy and certificates as part of the software installation. This enables NetScreen-Remote software to be deployed with traditional software-distribution systems (such as Microsoft SMS) or login scripts, or placed on a web site or drive-share for users to install over a network. Additionally, it is possible to launch other installers after the installation of NetScreen-Remote – this is useful when deploying NetScreen-Remote with third-party Anti-Virus or Personal Firewall software without having to install multiple applications individually.

The NetScreen-Global PRO management system will automatically create VPN policies for NetScreen-Remote users. VPNs are defined from within the NetScreen-Global PRO Console by the Administrator and applied to users or user-groups. Server-Side TLS (128bit SSL) is used for out-of-band user authentication and policy transfer to NetScreen-Remote clients. Upon a connection, the NetScreen-Remote client will use PKI to authenticate the NetScreen-Global PRO server, eliminating the possibility of a man-in-the-middle attack against the Global PRO system. Only if the Global PRO system itself is valid will the user’s login and password be submitted.

NetScreen-Global PRO will first attempt to authenticate the user, via the built-in user database or an external LDAP or RADIUS System (Global PRO 3.1, Target Availability Q2/CY02) After the authentication is successful the user’s policy is securely downloaded to their machine (Figure 4-
1.) Since authentication to the Global PRO system occurs prior to policy download, you are assured that only valid NetScreen-Remote users are able to download VPN configuration and that users are always receiving the latest VPN policy. Furthermore, as VPN policies are applied to users, as opposed to machines, a NetScreen-Remote user will always gain the same access rights from any machine running NetScreen-Remote in the world. This also simplifies the configuration, as the Administrator need not worry about applying access rights to machines, only users or user-groups. The VPN policy is locked when downloaded from NetScreen-Global PRO, which prevents end-users from tampering with configuration or keys. If a preshared or manual key is used, it will be obfuscated in the registry so that it cannot be viewed.

Central Policy Management—Global-PRO

Step 1: NetScreen-Remote first authenticates Global-PRO Device itself via Server-Side SSL then Sends username & password of secure channel, upon successful authentication VPN Policy for Remote user is downloaded securely over SSL Channel

Step 2: IPSec VPN Connections may now be initiated to NetScreen-Devices by Remote User

Figure 4-1: Overview of login process with NetScreen-Global PRO

Authentication to NetScreen-Global PRO provides VPN policy for remote user, after that the VPN is established to a NetScreen device.

When a user logs out of NetScreen-Remote, all VPN policy and keys are purged from the users machine. This eliminates the possibility of a lost or stolen laptop gaining access to VPN or configuration information. It also ensures that the user must authenticate to the NetScreen Global PRO system prior to accessing the VPN, leading to a more controllable remote access solution.

NetScreen-Remote must be configured to talk to NetScreen-Global PRO. The default.ang file on the NetScreen-Remote install directory tells NetScreen-Remote how to contact the NetScreen-Global PRO system (IP Address or Hostname) what Policy Domain the client will login to, and various timeout and reconnect values used for redundancy. Multiple NetScreen-Global PRO systems may be specified in the default.ang file when using multiple systems. If the NetScreen-Remote client is unable to contact the first server before the timeout interval, it will attempt a connection with additional servers. Default.ang will always be used as the default profile; however multiple configuration files with *.ang suffix may be created in the install directory, each will become a separate profile from which the user can select between. This enables NetScreen-
Remote users to connect to separate several different Global PRO systems or policy domains. If the user does not specifically select which profile to use, the default.ang will be used. Since ANG profiles are copied to the user’s machine upon installation of NetScreen-Remote, no additional configuration is necessary by the end user – they simply install NetScreen-Remote and launch the login program when they wish to connect to VPN resources.

Once NetScreen-Remote software has been installed, it will automatically check for updates and newer versions upon each login to the NetScreen-Global PRO system. This update process occurs over the SSL channel prior to the VPN Policy download. If a newer version of a file is available, NetScreen-Remote will only download the specific files that have been updated. Since the update process is automatic, users will always using the latest software without any manual intervention.

In some cases it may be desirable to distribute a default VPN policy file with NetScreen-Remote. Typically this is done in environments without NetScreen-Global PRO. A VPN policy file named “default.spd” may be placed in the NetScreen-Remote install directory. Upon installation this VPN policy will be installed on the client until another policy file is loaded. Policy-files can be loaded into NetScreen-Remote simply by double-clicking on the file, or running a command-line argument from a batch file or website. If using preshared key without NetScreen-Global PRO the Administrator must create a unique VPN policy file for each user. This is done with the Security Policy Editor on the Administrators machine. For Certificate-based VPNs using Group-IKE ID, it is possible for multiple users with the same access policy to share a common policy file. If desired this policy file may be saved without a preshared key or locked by the Administrator. For more information on configuring this refer to the NetScreen Concepts & Examples guide and the NetScreen-Remote Administrator Guide.

It is also possible to distribute and install a CA certificate with the NetScreen-Remote installation. This is advised when deploying X.509 Certificate authentication for the first time. NetScreen-Remote 7 adds support for the Microsoft Crypto API (MSCAPI). With MSCAPI, each user is given a Personal Certificate Store and certificates may be loaded via simply double-clicking on a certificate file or loading from web-browser. Any certificate on the machine may be used for IKE by NetScreen-Remote, simplifying the deployment and management of user certificates. Certificate files (*.CER) may be placed in the NetScreen-Remote install directory and will be installed on the users machine during setup. A CA Certificate will likely specify a CRL path, which NetScreen-Remote will check for certificate revocation purposes.

Summary

Remote access is essential for any company that needs to enable secure access to internal servers or networks for mobile workers or business partners. VPNs have proven to be a cost effective, secure and scalable way to deploy remote access. NetScreen products give the Administrator the flexibility to use multiple VPN technologies and authentication systems while providing secure and scalable remote access. With the NetScreen-Global PRO management system, NetScreen is redefining how VPNs are deployed by moving away from configuring individual devices and users and moving to a policy-based model where VPNs are centrally defined and applied to devices and users. This greatly simplifies initial deployment and ongoing management of remote access VPNs of any size.

NetScreen’s flexible product offering provides cost-effective solutions for networks of any size. From the NetScreen-5XP to the multi-gigabit NetScreen-1000, NetScreen provides a wide breadth of devices to support the bandwidth requirements of organizations of any size, from 10 to 10,000 active remote users. NetScreen Global PRO is available at many price-points, depending on the number of devices you wish to manage. The NetScreen remote access solution enables straightforward deployment, a clearly defined upgrade path and support for industry standard VPN and authentication technologies.