WHITE PAPER

SSL vs. IPSec

Streamlining Site-to-Site VPN Deployments

May 2011

Introduction

Traditionally, corporate users rely on IPSec for site-to-site access. However, the deployment of IPSec has never been easy due to complications from corporate firewalls, network address translation (NAT) and the complexity of the IPSec protocol itself. In certain instances, these challenges have made establishing an IPSec site-to-site connection painful if not downright impossible. An example being, a deployment scenario wherein one network location needs to make specific resources available to partners or outside contractors, yet also needs to securely protect other resources located on that same network. This requires complicated access control lists (ACLs) to be configured on each site. This is not only time consuming and cumbersome but also provides administrators plenty of opportunities to make mistakes that could lead to a security breach. In addition, with IPSec deployments, IP conflicts are inherent and force administrators to configure and maintain NAT rules on both sides of the network to prevent these conflicts.

To address these challenges, and to address challenges with other common scenarios including application outsourcing, mergers and acquisitions and delivery of hosted services, Array Networks has introduced SiteDirect, the industry's first and only site-to-site SSL VPN solution. This software product, available on Array's line of SPX Series Universal Access Controllers, leverages SSL's proven security and ease of use, and runs on a higher network layer (TCP or UDP) to easily traverse firewalls and NAT devices without any network topology changes. SiteDirect uses revolutionary and patent-pending resource publishing and identity-based access control to grant logical levels of resource access while hiding all internal network destinations. Only that which the remote site needs to access is exposed, nothing more. User-level granular control makes it simple for administrators to specify who can access resources. Any potential IP conflict is automatically resolved through SiteDirect's unique dual NAT on both end of the site-to-site tunnel.

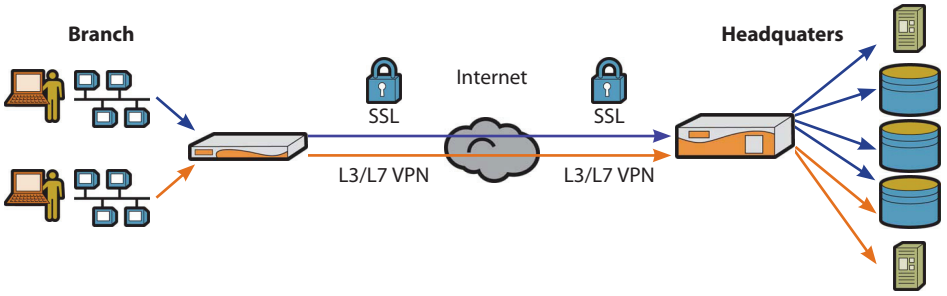
As a software product for Array SPX Series Universal Access Controllers, SiteDirect supports the ability to operate in conjunction with identity-based access control as well as remote access SSL VPN from a single integrated platform. As a site-to-site alternative or replacement, this offers tremendous flexibility in supporting secure site-to-site access that spans user, application and network level connectivity. What's more, SiteDirect's integration with the network is seamless and requires no changes to site topology, firewall ports and ACL mapping. Easy to set-up and manage, SiteDirect automatically avoids IP conflicts and can be quickly configured from via an intuitive WebUI.

The following is a comparison between IPSec and Array's SiteDirect site-to-site SSL VPN solution:

	Array SiteDirect™	IPSec
Public IPs	Only one site	Both sites need public IPs
Firewall	SSL is allowed by default	Need to open firewalls for IPSec traffic
NAT Devices	No changes	Need to deploy NAT traversal techniques and no guaranteed success
Resource Control	Only needed resources are exposed, i.e. Application Level Control	All resources on the network is exposed and requires complex ACL management.
User Control	Authorization and Authentication	None
IP Conflicts	Automatically Resolved	Complicated NAT and IP Mapping required

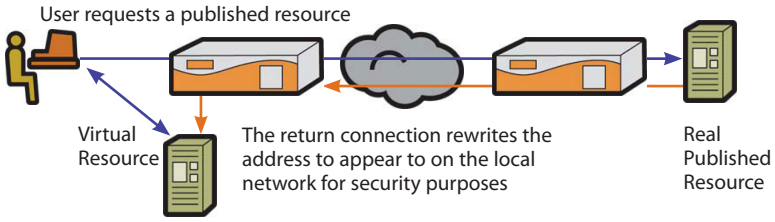
How It Works

With SiteDirect, application-level access is bi-directional where either side may initiate the connection with SSL tunneling on demand (or select to have an always-on tunnel).



Administrators may specify which network resources and applications specific users (e.g. contractors, partners, or customers) can access through resource publishing. To achieve the highest level of security, SiteDirect hides the published resource's original network address and assigns new network addresses on the client side of network so it appears as though the resource is on the local network.

Any resource (service, host or network) that needs to be published is configured on the SPX on the resource side of the network. The resource-side SPX then informs the client-side SPX of the published resources. Administrators need to also estimate how many clients on the client side network are going to access the published resources, and reserve the required number of IP addresses on the resource side network to accommodate these clients.



The client-side SPX provisions an IP address range for the published resource on the client side network. The client side SPX provisions a fully qualified domain name for the resources and resolves them to the provisioned IP addresses. Client computers on the client-side network have no knowledge of the resource-side network or its resources – all the clients see is a virtual application resource with a provisioned IP address on the client side network.

When the client-side SPX receives requests destined to a published resource, a secure tunnel is dynamically established on-demand with the resource-side SPX. SiteDirect provides an option to maintain a persistent connection so the SSL tunnel remains open once established.

Because there are no firewall ports to configure, no complex ACL mapping and no inherent IP address conflicts, SiteDirect is significantly easier to deploy and maintain than traditional IPSec solutions. What's more, SiteDirect offers fine grain access control, end point security and supports enterprise-class scalability. A revolutionary new alternative to IPSec VPNs, SiteDirect offers the highest degree of security by leveraging Array patents in resource publishing and identity-based access control to create logical level of resource access while hiding and protecting the details of all internal networks.

SiteDirect Concepts

Resource Publishing

Resource publishing specifies resources which can be made available to remote sites and users. Resources may consist of applications, hosts and/or networks. These resources may be made available in one of the two ways: NAT/PAT (Port Address Translation) Mode or Transparent Mode.

NAT/PAT Mode hides the real IP addresses of both the source (client-side network) and destination (resource side-network) using a DHCP mechanism or a static IP pool to assign local IPs addresses and thus avoid IP conflicts. This mode may not support applications with embedded IP addresses.

Transparent Mode allows the remote client to have access to the real network IP addresses of the published resource as opposed to concealing this from the client. This works like traditional IPSec VPN where the real IP addresses of the source and destination are used and care must be taken to avoid address overlap conflicts.

Point-to-Point Deployment

The point-to-point deployment makes a specific resource (or group of resources) available between two sites/peers. For example, linking a corporate office with a regional partner office and allowing each location to have access to the other's mail servers.

Hub and Spoke Deployment

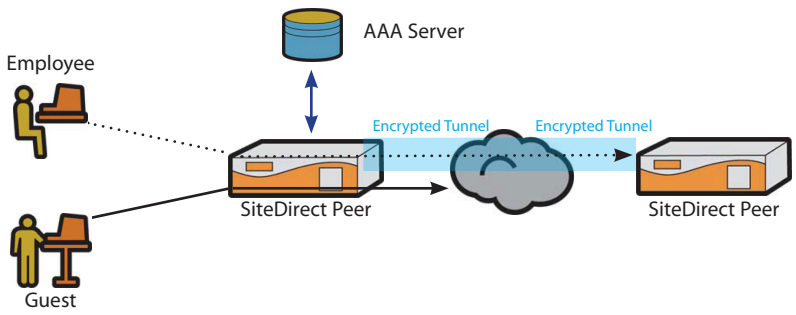
The hub and spoke deployment makes a specific resource (or group of resources) available to multiple peers, but does not allow those peers to gain access to each other. For example, a corporate office allows three regional partners offices to access the corporate application server, but not allow the regional partners offices to have access to each other offices.

GRE (Generic Routing Encapsulation)

SiteDirect publishes resources (including networks) from one end of the secure tunnel to the other granting fine grain access to resources; however, SiteDirect does not pass. In order to send broadcast/multicast IP packets and non-IP packets between two remote sites through the SiteDirect tunnel, GRE must be utilized as SiteDirect cannot tunnel these traffic types directly.

ATF (Authorized Traffic Forwarding)

ATF is a clientless access control method used to authorize traffic before the SPX forwards it. There may be several types of end users such as guests, contractors, employees (even employee department groups such as finance or engineering, etc.) where different users have different access rights to different resources (servers, files, etc.). In this clientless access mode, the SPX would act as a gateway, forwarding packets "to" and "from" destinations based on authentication and authorization rules. While using ATF together with SiteDirect, administrators will be able to force the users to login to the local SPX before they can access the resources published from the remote site.



SiteDirect FAQs

Q: Is the SiteDirect feature available on every SPX model?

A: Yes, customers must purchase an SPX appliance, along with SiteDirect and the desired number of site-to-site peers.

	SPX800	SPX1800	SPX2800	SPX4800	SPX5800	SPX6800
# of Peers	1	5	25	50	250	250

Q: What is SiteDirect's value or differentiator?

A: User and application-level granular control makes SiteDirect easy to deploy, manage, and more secure than IPSec.

SiteDirect's deployment within the network is seamless and requires no changes to either sites' topology -- no firewall ports to setup, no complex ACL mapping required, automatically avoids IP conflicts and can be quickly configured from the WebUI thus reducing costs and IT management overhead while offering greater flexibility and ease of migration/integration of remote or new sites.

SiteDirect's differentiator is patent-pending resource publishing technology which allows administrators to control what the remote site can access at the application level. ATF technology enforces user login before they can access published resources

Q: What protocols are supported by SiteDirect?

A: All IP based protocols are supported by SiteDirect.

Q: Does SiteDirect support broadcast or multicast?

A: SiteDirect does not pass broadcast/multicast IP packets or non-IP packets though the secure tunnel. However, GRE over SiteDirect may be utilized to transmit traffic, regardless of type, as long as this traffic is supported by routing devices.

Q: How does SiteDirect prevent IP conflicts?

A: SiteDirect dynamically assigns IP address from local DHCP servers or predefined IP pools. SiteDirect automatically performs NAT on each site's SPX to make certain that resources or user connections are using the assigned local IP addresses. Administrators may choose to use existing DHCP servers, allocate an IP pool or statically assigned IP addresses. Transparent mode can be used if there is no IP conflict issue or when it's desired to have the remote site see the actual IP address.

Q: Does SiteDirect work together with L3 remote access VPN?

A: Yes. An off-site user may take advantage of L3 VPN (Network VPN) to connect to the client site and then access the resources published from a remote site. This is very useful when a user wants to access a site-to-site resource while the user is outside the client site.

Q: Can SiteDirect enforce user login before they access the peer site?

A: Yes. With ATF technology, administrators can enforce user login before users can access published resources making certain that only authorized resources are available to users.

About Array Networks

Founded in 2000, Array Networks is a global leader in enterprise secure application delivery and universal access solutions. More than 5000 customers' worldwide – including enterprises, service providers, government and vertical organizations in health care, finance, insurance and education – rely on Array to provide anytime, anywhere secure and optimized access. Industry leaders including Deloitte, Red Herring, Gartner, and Frost and Sullivan have Recognized Array as a market and technology leader.

May-2011 rev. a

Corporate Headquarters

Array Networks, Inc.
1371 McCarthy Blvd.
Milpitas, CA 95035
408-240-8700
1 866 MY-ARRAY
arraynetworks.net

ASIA Headquarters
Array Networks China (Beijing) Corp., Inc.

Liang Ma Qiao Road,
Chaoyang District,
Beijing, No. 40, the
Twenty-First Century,
10-Story Building,
Room 1001-1017
Post Code: 100016
+010-84446688

EMEA Headquarters

Array Networks UK
4 Cross End
Wavendon
Milton Keynes
MK178AQ
+44 (0) 7717 153 159

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866 MY-ARRAY (692-7729) or authorized reseller.