

Array SiteDirect™ Frequently Asked Questions

Overall Functionality

What is SiteDirect™? What is Resource Publishing?

SiteDirect™ is a unique, patent-pending technology that extends the SSL VPN paradigm to site-to-site deployments. SiteDirect's Resource Publishing technology securely exports the application to the user, without combining two networks into one. This is the only solution that provides secure application access to users and organizations without exposing the topology of their internal network.

Why hasn't anyone used SSL to deploy site-to-site up to this point? Is it hard to do?

Array's SiteDirect™ provides much more than basic site-to-site VPN functionality. SiteDirect™ is the result of technical innovations that extend the benefits of SSL VPN technology – secure application publishing, network opacity, flexibility, and ease of use – to the branch office and the partner office. Array is the first and only vendor to provide remote access and site-to-site access on a unified SSL VPN platform specially designed for the needs of a highly distributed, interconnected, and rapidly evolving global enterprise networking environment.

How does Resource Publishing work?

The resource (application, host, or network) to be published is configured on the SPX on the server side network. The server side SPX informs the client side SPX of the resource to be published. The client side SPX provisions an available IP address for the published resource on the client side network. The client side SPX provisions a fully qualified domain name for the resource and resolves the name to the provisioned IP address. Client machines on the remote network are not allowed access to the local network – all they see is a virtual application server at the provisioned IP address.

Why is this different and better than IPSec?

Array's SiteDirect technology provides superior security and flexibility compared to IPSec products. IPSec VPNs are designed to connect two networks into one. Array's Resource Publishing securely exports applications to remote users without exposing the topology of the internal network. Users and organizations can get access to the applications that they need without being allowed onto your internal network.

In addition, *SiteDirect* provides unparalleled flexibility and ease of configuration for deployment in rapidly changing network topologies. All traffic is tunneled on port 443, eliminating firewall traversal and tunnel NAT complications. New tunnels can be easily configured without affecting existing network infrastructure or services. Dynamic provisioning of resources allows IP conflicts to be resolved without sharing network topology information. For example, this flexibility is ideal for partner and customer access, as well as mergers and acquisitions.

Does *SiteDirect* support all IP applications, similar to IPSec?

Yes.

In a trusted network scenario, can you just open up the entire network to the other side without doing a lot of manual configuration?

Yes. *SiteDirect* also provides network level connectivity equivalent to IPSec VPNs. This can be done by publishing the entire local network in transparent mode.

Does *SiteDirect* provide the security protection that IKE provides on IPSec devices?

When an SSL session is established, both endpoint SPX devices authenticate each other and session keys are exchanged. This functionality is similar to that provided by IKE, and is built into the SSL protocol.

How do you provide the equivalent of Security Associations (available in IPSec)?

The SPX allows up to 256 independent virtual sites to be configured on a single system. Each virtual site can be configured with its own security properties, including keys, certificates, cipher suites, and authentication settings.

How does performance compare with IPSec?

Array's *SiteDirect* is designed to provide performance comparable to equivalent IPSec devices on the market. *SiteDirect* uses the same SpeedStack technology as Array's remote access SSL VPN, the fastest SSL VPN in the industry.

Do you have an integrated firewall?

SiteDirect is not intended to act as a firewall or intrusion prevention system. The SPX can be deployed in front of external firewall and intrusion prevention appliances. Alternatively, the SPX can be deployed without an external firewall, since it is built on a hardened operating system that is designed to protect the SPX and the resources behind it from network attacks.

What are the advantages of using SiteDirect over using remote access SSL VPN from a partner office or branch office?

SiteDirect allows users at a partner office or branch office to access published resources without having to manually log into an SSL VPN gateway. Users can access all IP-based applications from any client machine, regardless of the client operating system or the user's administrative privileges on the client machine. SiteDirect also allows machines at the remote office to communicate with the published resources without any human intervention. All of this can be done without exposing the topology of the internal network to users at the remote office.

The advantages of remote access SSL VPN are that it authenticates individual users, enforces access controls based on user identity, and restricts access based on endpoint security checks.

Deployment

How do two sites establish a connection? How do on-demand and persistent connections differ?

By default, an SSL tunnel is established on demand. When the SPX receives traffic destined to a published resource, a secure tunnel is dynamically established.

SiteDirect provides an option to maintain a persistent connection. In this case, an SSL tunnel is established once SPX devices on both sites are up, and the tunnel remains open as long as keep-alive packets are received by SPX devices on both sites.

The range of applications supported in both cases is the same.

How do the two gateways authenticate?

SPX gateways can authenticate each other using SSL certificates. When a SiteDirect tunnel is established, each SPX validates the other's SSL certificate as part of the SSL session establishment process. On the server side SPX, the administrator must import the root certificate of the issuer of the client side SPX's certificate. The administrator may optionally choose to configure the server side SPX to accept only client certificates with certain attributes in the specified fields (e.g. C=US, O=Array Networks). In addition, the server side SPX can optionally validate the certificate of the client side SPX against a local database or an external LDAP server.

Alternatively, the client side SPX can authenticate itself by username and password. The server side SPX can validate the credentials against an external authentication server (Active Directory, LDAP, RADIUS) or against the locally configured credentials.

No manual intervention is needed with either authentication method.

What encryption protocols and ciphers are supported, i.e., 3DES, AES, etc.?

SiteDirect supports all encryption protocols (SSLv3, TLSv1) and ciphers (including 3DES, AES, and RC4) that are supported by the other SPX access methods.

How are keys generated and handed out (i.e., IPsec uses PKI keys)? Does it require pre-shared keys?

Key generation and distribution is controlled by the same technology that is used for remote-access SSL VPNs and SSL-enabled Web servers. Pre-shared keys are not required.

On each site, a key pair (consisting of a private key and a public key) is generated on the SPX. The private key is a secret that is stored on the SPX. The public key is used by other devices to encrypt traffic to be sent to this SPX; the encrypted traffic can only be decrypted by this SPX using its private key. Using this key pair, the SPX generates a Certificate Signing Request (CSR) that can be used to obtain an SSL certificate from a trusted Certificate Authority (CA) such as Verisign. The certificate must be imported into the SPX. (It is also possible to generate a certificate on the SPX itself for testing purposes).

When an SPX establishes an SSL tunnel with a peer SPX, it obtains the peer SPX's certificate containing the peer's public key. This certificate exchange is a built-in part of the SSL protocol.

What types of resources can be published? How are the resources identified?

A published resource can be an application (defined as a host and port number), a host, or an entire network. A host can be identified either by name or IP address. For example, an internal Web site can be published as a service using its internal hostname and port 80. A network is identified by its IP address and netmask.

Can SiteDirect support applications where both endpoints act as servers? For example, how can SiteDirect be configured to allow two offices to exchange email?

Yes, applications that initiate connections in both directions are supported by publishing resources in both directions. To support secure email between two sites, the SPX at each site must publish the local email server to the other site. To provide full two-way connectivity between networks at two sites, the SPX at each site must publish the local network to the other site.

Is DHCP supported?

Yes. SiteDirect integrates seamlessly with existing DHCP infrastructure. When a remote resource is provisioned to the local network, the local SPX obtains an available local IP address from the configured DHCP server to provision the resource. Client systems on the local network will then use the local IP address to communicate with the published resource.

SiteDirect can also provision resources locally by obtaining an IP address from a configured IP address pool. Note that provisioning resources using DHCP has the advantage of automatically avoiding IP conflicts.

How is DNS handled?

The SPX acts as a DNS server to resolve the provisioned hostnames of the published resources to their provisioned IP addresses. There are two ways to configure this.

The recommended approach is to use the client side SPX as a zone authority server for the published resources. On the SPX, enable the Local DNS feature, which allows the SPX to act as a DNS server listening for requests on the specified IP address. In the site-to-site configuration, create a domain (e.g. "vpn.company.com") and associate it with the site-to-site peer that is publishing the resources. If the peer publishes a resource with hostname "server", the resource will be provisioned on the client side network with FQDN "server.vpn.company.com". The SPX will automatically resolve this FQDN to the locally provisioned IP address of the resource. The administrator will need to configure the existing DNS server on the client side network to use the Local DNS on the SPX as the zone authority server for "vpn.company.com".

Alternatively, the client side SPX can be used as the primary name server on the client side network. In this case, the published resource can be provisioned either with an FQDN on the same domain as the rest of the client network (e.g. "server.company.com"), or an FQDN on a domain associated with the site-to-site peer (e.g. "server.vpn.company.com"). Enable the Local DNS feature on the SPX and configure the client machines to use the Local DNS on the SPX as their

primary DNS server. On the SPX, configure the existing DNS server as an external DNS server. The SPX will automatically resolve the hostnames of provisioned resources to the locally provisioned IP addresses. For other DNS requests, the SPX will act as a relay by forwarding the request to the external DNS server.

How is NAT handled? What type of NAT is supported, 1-to-1 NAT or PAT? How are IP conflicts handled?

Suppose a server is published from site A to site B. A local IP address is dynamically assigned to the server on site B's network. When a client on site B's network sends traffic to the provisioned server, a source IP address for traffic from this client is dynamically assigned on site A's network. One-to-one NAT is used in both cases. By dynamically obtaining available IP addresses from existing DHCP servers, *SiteDirect* automatically avoids IP conflicts without any administrative effort.

Resources can also be published using transparent mode. In this case, NAT is not applied, and the topology of the published network is visible to users on the remote site. It is up to the administrator to make sure there are no IP conflicts in this case. Networks must be published in transparent mode, while hosts and applications can be published either in NAT mode or in transparent mode.

Do you support OSPF, BGP or any other routing protocols?

The big advantage of *SiteDirect* Resource Publishing is that the topology of the internal network is not exposed to users on remote sites. When a resource is published, the remote SPX listens for traffic destined to the application, and automatically tunnels the traffic to the SPX on the local network. As long as the actual application server is routable from the server-side SPX, no additional routes need to be configured.

When two sites publish their networks to each other in transparent mode, the administrator on each site will need to add a route on the local router with the remote network as the destination and the physical IP address of the SPX as the next hop. No other manual routing configuration changes are required. *SiteDirect* automatically uses static routing on the SPX to route traffic to the remote network. The SPX does not use dynamic routing protocols.

Is there an option for everyone to login?

This option is not available when only *SiteDirect* features are enabled. Once a resource has been provisioned to the local network, all users on the local network have access to the resource, if permitted by the configured *SiteDirect* policies. Policies can be configured to allow or deny access based on the traffic specification (source IP and port, destination IP and port, and protocol).

It is possible to require all users to log in by configuring a virtual site inside the client side network with both remote access and *SiteDirect* enabled. In this case client traffic would pass through the remote access gateway before reaching the *SiteDirect* tunnel. It would also be necessary to prevent clients from connecting directly to provisioned resources, either by configuring *SiteDirect* policies or by configuring the network such that the provisioned resources are not routable from the clients.

Management

How is *SiteDirect* managed?

Like all other SPX features, *SiteDirect* can be configured using either the WebUI or the CLI. *SiteDirect* configuration takes advantage of the SPX's virtualization technology, which allows different services to be managed by separate administrators. With support for XML-RPC, a wide range of third party applications can be used to automate management tasks.

How are policies administered?

Policies can be configured to control access to published or provisioned resources. No knowledge of the internal topology of remote networks is needed. The policies are configured and stored locally on the SPX.

What kind of tools do you offer to monitor your tunnels?

The SPX supports monitoring of *SiteDirect* tunnels via statistics reported in the CLI and WebUI, as well as via SNMP. The information reported includes traffic statistics for open tunnels and published applications, statistics on authorized and unauthorized access, and other details useful for troubleshooting.

What logging and reporting capabilities are supported?

The SPX provides logging of *SiteDirect* events using the same framework that is used for all other SPX features. Log messages are generated using the standard WebTrends Enhanced Log Format. Messages are logged to an external syslog.

What tools do you provide to do end to end troubleshooting? How can I quickly identify the problem?

The SPX provides detailed logging of *SiteDirect* events to assist in troubleshooting.

How do you manage multiple boxes? What is the model for automating configuration management across a medium to large network with 10 to 100 nodes?

Each individual site (an SPX or a cluster of SPX units) must be configured independently. Configuration is automatically synchronized among redundant units in a cluster.

Integration

Can resources be published to remote access users who log into the SPX on the remote network?

Yes. Remote users connecting to a network using L3VPN will have access to the same set of published resources as internal users on that same network.

Can I support different customers and partners on the same *SiteDirect* box?

Yes. Up to 250 separate *SiteDirect* peers can be configured on a single SPX appliance.

If so, how do I make sure that the data is separated from each other?

Each partner will have access only to the specific resources that are published to them. If separate application services are published to two different partners, each partner will not have access to the application service used by the other partner.

If the same application service is published to both partners, the application will need to be able to authenticate each partner and enforce separation of application data.

How does Virtualization help?

Virtualization allows different services to be configured and managed by different administrators. For example, a separate virtual site can be created for each partner. Each virtual site would publish the appropriate resources required by the respective partner; each site would also have its own SSL and authentication settings and be managed by its own administrator.

However, it is also possible to support multiple partners on a single virtual site.

What about a small office appliance?

The SPX 2000i is our small office appliance product. It is intended for offices with 10-100 users and supports all *SiteDirect* features.

How do you handle WAN optimization?

SiteDirect is compatible with external WAN optimizers that modify traffic payloads without changing the IP headers. The WAN optimizer should be deployed between the SPX and the router, on both sides of the tunnel.

Appendix

Are *SiteDirect* resources available to remote access users via all access methods? Are there any limitations?

Resources published in NAT mode are accessible via all access methods. Web, file, clientapp, TCS resources must be configured using the hostnames of the backend servers.

SiteDirect networks published in transparent mode are accessible via L3VPN, Web, and File access methods. The Clientapp and TCS access methods are not compatible with transparent mode.

Are there any limitations on IP-based protocols or applications that can be supported?

The initial release of *SiteDirect* does not support multicast or broadcast traffic. Automatic discovery of Windows file shares on servers published from remote networks is not supported.

When resources are published using NAT mode, protocols such as FTP that embed IP addresses in their payloads are not supported in the initial release. Transparent mode is recommended for publishing applications that use these types of protocols. Note that dynamic-port applications that only embed only port numbers in their payloads are supported using either NAT or transparent mode.

For pure *SiteDirect* access, can access policies be applied based on user identity? Are there any other limitations?

No, access policies based on user identity are not supported in the initial release. Policies can be configured both on the server side SPX and on the client side SPX. The policies configured on each site are applied to the source and destination IP addresses visible to the local network.

For example, suppose site A publishes resources to site B. An IP range, IP-B, is provisioned for the published resources on B's network. An IP range, IP-A, is provisioned for the clients from site B on A's network. A policy on the SPX at site A can deny traffic from IP-A (representing users from site B) to local resources or subnets with specified IP addresses. A policy on the SPX at site B can deny traffic from clients connecting from specified IP addresses or subnets to IP-B (representing resources published by site B). Here is a summary of the types of restrictions that can be configured using SiteDirect ACLs:

SiteDirect Configuration	Server-Side Policies	Client-Side Policies
One virtual site, publish resources in NAT mode	Client Site -> Server IP	Client IP -> Server Site
One virtual site per resource, publish resources in NAT mode	Client Site -> Server IP	Client IP -> Resource
Publish resources in transparent mode	Client IP -> Server IP	Client IP -> Server IP

Suppose site B contains two subnets, B1 and B2. Suppose A publishes resources R1 and R2. Suppose we want to allow only users from subnet B1 to access resource R1 and users from subnet B2 to access resource R2. We can create two separate virtual sites, V1 and V2, on the SPX at site B. Create a single virtual site at A, and configure V1 and V2 as separate SiteDirect peers. Publish only R1 to V1, and publish only R2 to V2. Then R1 and R2 will be provisioned on different IP ranges on B's network. We can then configure policies on site B that permit clients with source IP's in subnet B1 to send traffic to the IP range for R1, and clients with source IP's in subnet B2 to send traffic to the IP range for R2.

For remote access users, can access policies be applied based on user identity? Are there any other limitations?

Yes. Remote access ACLs can be configured to restrict a user or group's access to published resources. Remote access ACLs take precedence over SiteDirect ACLs. Remote access IP ACLs apply to the L3VPN, Clientapp, and TCS access methods. Remote access HTTP and file ACLs can be used to restrict access to Web and file resources located on provisioned servers. If the servers are published using NAT mode, the servers in the ACLs should be identified using their provisioned hostnames. As in the case of pure site-to-site access, actual IP addresses of remote servers are not visible when NAT mode is used; only the local IP ranges associated with SiteDirect peers are visible.

Here is a summary of the types of restrictions for remote access users that can be configured using remote access and SiteDirect ACLs:

SiteDirect Configuration	Remote Access ACLs	SiteDirect Policies (Client-Side SPX)
One virtual site, publish resources in NAT mode	User/Group -> Server Site	Client IP -> Server Site
One virtual site per sources, publish resources in NAT mode	User/Group -> Resource	Client IP -> Resource
Publish resources in transparent mode	User/Group -> Server IP	Client IP -> Server IP

It is possible to require internal users to log in and enforce access control based on user or group identities by creating a virtual site on the internal client-side network and enabling both remote access and *SiteDirect* features.

Note: In some cases it is also possible to implement user identity based access controls using *SiteDirect* policies. However, this capability is limited since *SiteDirect* policies enforce restrictions based on the client's IP address, which is only associated with user or group identity when L3VPN is used. User-level access control is available only when static IP addresses are assigned to individual users. Group-level access control is available when client IP addresses for different groups are assigned from separate IP ranges. For access methods other than L3VPN, the client's IP address will be the inside physical IP address of the SPX. This means that *SiteDirect* policies will have no effect except to either permit or deny all such remote access traffic to the specified destinations.