Vidder SDP Managed Services

Service Descriptions and Options

June 2014

Table of Contents

Vidder SDP Managed Services

Software Defined Perimeters (SDPs)

The Extended Enterprise inverts all the assumptions that traditional hardware-based perimeter (firewall/VPN/IPS) solutions were designed around – that the internal network was secure and the Internet was insecure and thus security could be attained by creating a security perimeter between the two. Nowadays, the use of BYOD devices and guest devices internally, the success of phishing attacks at injecting attacker software on internal devices, the need to extend IT capabilities to contractors and outsourcers and other partners, and the trend towards the use of SaaS and Cloud computing /storage, have shredded pretty much every assumption that the previous generation of security tools were built upon.

Software Defined Perimeter (SDP) is a set of standards from the Cloud Security Alliance (CSA) that create a new intrinsically secure connectivity model to meet the needs of today's Extended Enterprise.

Detailed descriptions of SDP functionality can be found elsewhere. But basically it defines an "attest-before-connect" connectivity model.

In the SDP paradigm, "attest" means "make sure the user is who you think they are and coming from where you expect them, the device they are using is known to you, the software on that device that is associated with connecting to your application is unadulterated and you are isolated from compromises that may exist elsewhere on the device".

SDPs are created one application at a time. Each server that delivers the application starts in a DENY ALL state. Each device of each user that is authorized to connect to the application starts as an island, with no connectivity or even visibility to the application infrastructure.

SDPs create the links that connect the islands, stitching together connectivity one connection at-a-time as endpoints attest to their worthiness for such connectivity.

SDPs address many of the security and reliability issues that plague IP networks today:

- Resource and bandwidth starvation denial-of-service attacks
- Man-in-the middle attacks
- Browser compromises and cross-site attacks
- OS and Application vulnerability attacks
- Lateral movement essential to Advanced Persistent Threats

SDP Use Cases

Private Internet

The open architecture of the Internet results in a huge attack surface, which leads to Denial-of-Service attacks, Man-in-the-Middle attacks, and Vulnerability Exploits (e.g., SQL injections, XSS, CSRF, etc.) which, in turn, results in data theft, damaged reputation, and reduced reliability. These issues are rapidly becoming business disabling issues for high value applications such as supply chain Extranets, field workforce management, and mobile application back-end networks. These issues are also in many cases preventing Enterprises from taking full advantage of the advantageous economics of cloud computing, cloud storage, and SaaS.

Now, enterprises have a new technology option for protecting servers connected to the public Internet, an SDP-enabled Private Internet. A Private Internet allows application owners to disconnect servers from direct Internet access and use Vidder as a front end to render the application servers invisible and inaccessible to unauthorized users.

Vidder eliminates public information such as DNS names and open IP interfaces of web-based extranet portals that hackers use to attack sites. Private Internets mitigate the most devastating Internet-based attacks such as Denial of Service attacks, Man-in-the-Middle attacks, and OWASP server vulnerabilities.

Aperture Access

Contractors, consultants, offshore engineers, and business partners, whether remote or on-site, require more and more access to internal services in order to facilitate efficient business practices.

Providing access to high value applications that are inside the corporate perimeter to non-employees is a challenge. Providing VPN access to non-employees is too risky as they have too much access. As soon as external personnel have access inside a perimeter, it is very difficult to restrict lateral movement. Alternatively, using e-mail attachments leads to a chaotic exfiltration of information out of the enterprise.

Until now, there has been no good option for allowing access between the extremes of full network access (VPN) and no connectivity at all.

Vidder's Aperture Access solution provides an alternative strategy to today’s “All in” VPN technology by enabling precision access to specific IT assets and nothing else. Aperture Access can be used to create a locked down path to internal high value applications that cannot be re-tasked to an external network.

External users never see the true location of protected servers, nor do they have visibility to other servers and devices on the internal network, IP addresses, DNS/DHCP servers, etc., as the Gateway hides all that. They simply click on a desktop icon or phone/tablet app for precision access to authorized servers.

Providing access for employees to high value applications on devices not tightly controlled and managed by IT (BYOD) is a challenge similar to the issues of providing access to outsiders described above. You trust your employees but you can’t be sure of the trust of the consumer device they are using to connect to your IT infrastructure. Providing VPN access to BYOD devices is too risky as that provides attackers who have compromised the devices too much access. As soon as such attackers personnel have access inside a perimeter, it is very difficult to restrict lateral movement.

Vidder's Aperture Access solution enables precision access to specific IT assets from BYOD devices and nothing else. In this case other software on BYOD devices never see or have access to any internet systems other than the authorized services.

Vidder SDP Managed Services

SDP involves deploying several software components that operate in a highly coordinated manner to provide an intrinsically secure yet easy-to-use solution. But since many components are involved that may be geographically distant from one another yet need to be tightly coupled cryptographically, SDPs can be complex to deploy. Vidder SDP Managed Services make SDP capability and benefits available to customers with no need for the customer to become expert in the technology.

To deliver SDP Managed Services, Vidder utilizes internally developed SDP software combined with deployment automation tools to create a turn-key 100% up-time service operated by Vidder that can be deployed rapidly.

Each Vidder SDP Managed Service is single tenant. No part of the operational SDP system for Customer A is shared with Customer B. Such separation is critical for security purposes as well as to allow each solution to be optimized to meet each customer's needs. Each customer's SDP system is monitored and managed leveraging the Vidder Service Operations Center (VSOC).

Managed Service Functions Provided By Vidder

Solution Design

SDPs are fairly straight forward to design and implement. But there are some options related to the location of deployment of the various SDP software components, overall system scale and reliability, securely connecting SDP to the servers/application they protect, and how to integrate with existing Identity Management systems, that require some considered design choices. Vidder works with customers to create a design that is optimal for them.

Solution Deployment

Once the design is in place, Vidder creates, coordinates, and executes a project plan to deploy the target system so that the customer can enjoy the benefits of SDP as soon as possible.

User/Device On-Boarding and Support

The power of SDP is rooted in the deployment of per user and per device cryptographic elements that create a signature for them that differentiate them (the desired application users) from the rest of the world (attackers, Bots, malware, etc.). Vidder works with customers to identify the desired users and to on-board them onto the system.

Configuration Management

Vidder configures the initial system but also takes the responsibility for on-going configuration management as new features are turned on, as customers make changes to their Protected Server locations or firewalls, as the system is expanded to increase capacity, etc.

Security Management

Once deployed, Vidder provides on-going security management to ensure that the system provides the same benefits years after being deployed as it did day one. This involves assessing attacks, continually upgrading software, and executing "moving target" changes to system configuration parameters to continually frustrate attackers.

Availability Management

The services that Vidder SDP protects are generally high value services that often have some role in revenue-generation for Vidder's customers. 24x7x365 availability is the goal. One of the key values of SDP for certain Use Cases is protection against Denial-of-Service attacks. But protection against network failures, server failures, software failures, etc. is equally important. Every production solution

system Vidder deploys has redundancy built-in. But Vidder continually monitors the health of every system component as well as the end-to-end path and creates new instances as needed to ensure 100% uptime.

Aligning money with mouth, Vidder accepts penalties if that goal is not met.

Performance Management

Security is great … but not if it impacts performance, user experience, or business velocity.

The SDP core concepts and core architecture were developed to ensure that user experience and overall system performance are not impacted by the introduction of great security. But still, stuff happens. Vidder continually monitors overall system performance as well as each SDP element's resource utilization to ensure that such stuff doesn't happen to Vidder SDP customers.

Update Management

One thing about security software – it is never done - new innovations, new integrations, responses to new threats, performance or availability enhancements, new features all come pouring out of Vidder's development group on two week intervals from their Agile development process. Most of these enhancements can be introduced transparently into existing customer's environments with no effort needed by the customers or their users. In those cases, Vidder executes continual software enhancement.

In cases where users need to be involved or a short system outage is required, Vidder coordinates that activity with our customers.

Vidder SDP Service Delivery Architecture

The Vidder SDP Vidder service delivery architecture encompasses three major functional areas:

1. Functional SDP components that meet the SDP specification and add value beyond the specification. This includes SDP Controllers, SDP Gateways, SDP device Applications, and On-Registration/On-Boarding servers.
2. Deployment automation software that creates instances of the above components in the quantity and at the locations needed to meet specific customer needs.
3. Service Operating Venter software to enable remote provisioning, configuration, monitoring, and management of each deployed customer system.

Functional SDP Components

The Vidder functional components can be deployed in the cloud, at hosting centers or on customer premise as needed to meet the needs of each customer.

Software Characteristics

As one of the main contributors to the SDP specification, Vidder SDP software meets all SDP specifications, is compatible with specification-compliant client applications, and adds exceeds the capability defined by the standard in many important ways.

The software has been developed using and exceeding state-of-the art Secure Software Development Lifecycle (SSDL) practices and has been developed with-in a highly secure and battened down internal IT environment.

Each of the individual components of the SDP solution have been hardened at the Ubuntu 12.04 OS kernel level (using grsecurity) as well as at all layers above to enhance the security robustness delivered by the overall SDP architecture.

Highly Reliable and Scale-able Deployment

The starting configuration for all Vidder SDP deployments is 2:2:2:1, meaning 2 SDP Gateways, 2 SDP Controllers, 2 Databases, and 1Registration/On-Boarding Server (not needed for on-going operation).

All of these components can be deployed in the cloud, at a hosting center, or on a customer premise.

When deployed in the cloud, using AWS as the example, the redundant components are deployed within different Availability Zones and are deployed leveraging AWS Security Groups and VPC.

When deployed at Amazon, Vidder Managed Services uses the Amazon Relational Database Service (RDS). RDS servers are deployed in different availability zones within the same region to support high availability

When deployed on customer premises or in hosting centers, Vidder Managed Services uses DRBD on VMware vSphere systems using multiple machines.

Depending on the throughput, reliability, and geographic requirements, more Controllers and Gateways can be added to the solution as needed.

Deployment Automation

A Chef-based Provisioning server creates and configures SDP instances on an SDP-by-SDP basis basis to create the complete, tightly coupled, and pre-tested SDP deployment optimal for each customer's need.

Users and their devices are on-boarded using a Registration/Onboarding server. The Registration Server serves as a platform for the distribution of the SDP App and related PKI certificates for approved users.

The users access the Protected Service they are authorized for through the Vidder SDP App downloaded and installed as part of the on-boarding process.

Service Operations Center

Vidder maintains a Service Operations Center (SOC) at Vidder Headquarters in Campbell, CA that monitors the overall service and provided a central point of administration.

Monitoring and diagnostic tools provide real-time and historical visibility into the health, performance, and security of each system deployed for each customer, alert probable or actual incidents, and report on SLA achievement.

Monitoring capabilities at the SOC include:

- At a glance view of the health and configuration of all active SDPs and SDP instances (CNTLS, GWs, Registration Servers).
- Real-time monitoring is used for every SDP instance for the following parameters:
    - Disk space
    - Total load on the instance
    - Total Processes
    - SSH Users
    - Instance corruption
    - Zombies
- SysAdmn GUI for each SDP – present active user map, real-time and historical meters and graphs, filterable event logs, all configuration settings
- Status of Incident Response activities and resolutions
- Enabled/Disabled notifications
- Scheduling queue

Administrative tasks executed at the SOC include:

- Configuration management of all SDPs – add Protected Services and/or Servers, add SDP instances, changes secure backhaul configuration parameters, change Identity Management integration settings,
- Schedule of checks on services
- Enable / Disable cloud instances
- Schedule downtime on the host
- Create custom availability reports
- Building/launching of new SDPs

Data Reliability and Security Model

No Shared Configuration or Derived Data

SDPs are created on a single tenant basis for each Protected Service. No configuration data or reports or alerts or events or any such derived data is shared between SDP instances. Customers can choose to support multiple Protected Services from a single SDP but that choice is usually taken when all services are controlled by a common owner and there is little concern about configuration and derived data sharing among those services.

Encrypted-At-Rest Configuration and Derived Data

Even though there is little to no risk to exposure of SDP configuration or derived data even if made publicly accessible, you never know for sure how someone could take advantage of information about internal IP addresses or connection patterns or authentication policies. Therefore all this data is encrypted in the SDP Databases and only decrypted and used by the Controllers as needed in real time.

The Controllers, Gateways and Databases are also operating on security-hardened Operating Systems that are tightly controlled and managed by Vidder.

No Application Data Visibility

Customer application data is encrypted from the SDP App (on the initiating device) to the Gateway. In most secure backhaul configurations the data is also encrypted from the Gateways to the Protected Servers. There is a moment within the Gateway memory where the data is in the clear as it passes from one encrypted TCP connection to another. However, customers running HTTPS for their applications will still benefit from that level of encryption protection end-to-end, getting another level of encryption protection due to the additional encryption executed by the SDP. Vidder will have no visibility into such data nor will any attackers or customer running over the same internet links or operating in the same cloud environment.

No Access to Passwords

As discussed in a later section, in most cases, the Vidder SDP system does not store or use User passwords. In the default mode of Authentication (Transparent SDP MFA), device authentication is performed completely independently of user authentication. The SDP is only using device and software information that it configured as part of the On-Boarding process to determine whether a device/user is a candidate (SDP authorized device) for proceeding further into the overall system authentication process.

In the SAML Federation Mode, the Controllers simply wait for confirmation from other systems that user authentication has succeeded. Again, no passwords or sensitive user information are needed by the Controllers and therefore not configured and stored.

SDP Deployment Options

SDP Instance Numbers

The number of Gateways and Controllers deployed can be adjusted on an SDP-by-SDP basis to meet the needs of that specific application.

The number of Gateways needed is usually tied to the bulk peak throughput required of the system. Throughout depends a lot on the resources of the underlying processor and memory as well as on-going performance enhancements by Vidder engineers. As of now we dimension systems based on a conservative estimate of 500 Mbps peak throughput per Gateway.

The number of Controllers needed is usually tied to the peak sessions-initiated per second (basically the peak number of people launching their SDP App per second). Authentications depends a lot on the resources of the underlying processor and memory as well as on-going performance enhancements by Vidder engineers. As of now, we dimension systems based on a conservative estimate of 50 sessions-initiated per second per Controller.

SDP Instance Locations

Controllers, Gateways, Databases, and Registration servers are deployed and configured to work in a highly coordinated manner to deliver all the benefits of SDP. But there is no real architectural or topological dependency between these SDP components that limits where they can be deployed.

The only fundamental limit is that the various components be routable to one another. SDP Apps need to be able to route to SDP Controllers and Gateways, SDP Gateways need to be routable to SDP Controllers, etc. In practice this is rarely a limitation.

Many customers prefer that both the Controllers and Gateways be deployed in the Cloud somewhere. One motivation for that is that the Protected Service may also be in the Cloud (such as an Enterprise application that has migrated to the cloud, a B2B SaaS service operating in the Cloud, or a Mobile Application back-end). In that case, it is usually desired to deploy the SDP components in the same Cloud or Clouds as the Protected Service.

There are other situations where deployment of some or all of the SDP components in the cloud is desirable, even if the Protected Servers are not in the cloud. Denial-of-Service protection, for example, is optimized when the SDP components are delivered in the Cloud because they are connected to the massive bandwidth of the Cloud providers, and Vidder can leverage the elasticity features in the cloud to add Controller or GW instances to address peaks of load or to shift them to new addresses or location to create a “moving target” for the bad guys while maintaining connectivity for the desired users.

Even in the cloud, there are a lot of options related to Cloud Providers, Regions, Availability Zones, etc. that can be used to create a global footprint for an SDP that can operate independent of the health (or present pricing) of any particular provider.

There are good reasons, however, to consider deploying some or all of the SDP components on premise or at a hosting site. It reduces any costs or complexities associated with deploying Secure Backhaul (next section). It can allow the SDP system to operate primarily on a company’s internal network, which can make sense if most of the users are employees or other internal users. And it allows the value of other internal security controls such as data-at-rest controls, VLANs/subnetting, firewall and application firewall settings, etc. to be maximally leveraged.

Vidder can provide the same level of Managed Services whether the SDP components are deployed in the cloud, on premise, or some of each. We are happy to discuss the pros and cons of the various options and deploy and support the systems that result from that decision-making process.

Secure Backhaul Options

SDPs act as a front-end for applications to absorb the Denial-of-Service, Man-in-the-Middle, and Vulnerability Attacks they would otherwise be subject to and not optimized to thwart.

Often, it is not ideal for the Gateways providing the SDP protection to be co-resident with the Protected Servers. For example, it might be optimal to have the Gateways deployed in the cloud to benefit from the low cost, elasticity, and large bandwidth available in the cloud (to help defeat DOS attacks), while the Protected Server is at a customer premise that provides physical protection and secure connectivity to other local servers.

Even if they are co-located at a cloud site, the multi-tenant nature of the cloud site makes it valuable to secure the communications from the SDP GW to the Protected Server from others sharing the same Virtual Switch infrastructure.

Thus secure backhaul techniques are needed to provide a path from the Gateways to the Protected Servers that augment the value of the front-end SDP. Some options include:

- Simple FW rules on the Protected Servers so they only accept packets from SDP Gateways.
- Above, plus fixed TLS connections from GWs to Protected Servers (to maintain end-to-end encryption)
- Site-to-Site IPsec VPN connections from GWs to Protected Servers.
- MPLS

Authentication and Authorization Options

Vidder support several methods for performing authentication and authorization.

Transparent SDP MFA (Default)

In this default mode of Authentication (Transparent SDP MFA), device authentication is performed by the SDP and user authentication is performed independently by the application back end.

To perform its role, the SDP is only using device and software information that it configured as part of the On-Boarding process to determine whether a device/user is a candidate (SDP authorized device) for proceeding further into the overall system authentication process.

SDP User Authentication and Authorization

In this mode, the SDP executes Transparent SDP MFA (as above), but also requests and examines something that only the authorized user should know – a password or a PIN, before allowing a user into the SDP. Further user authentication may or may not be performed by the back end in this case.

SAML Federation

In this mode, the SDP executes Transparent SDP MFA (as above), but then coordinates a SAML based Federated Identity Process in order to (a) get confirmation via SAML that the User has been authenticated, and (b) gain access to Groups information that the SDP can translate to authorized services, before allowing connection into the SDP and to the authorized Protected Service(s).

Service Level Agreements (SLA) Options

SLA Level	Basic	Premium
Service Uptime	99.95% accessibility No outage > 6 hours (after notification)	100% accessibility Fee rebate per day an outage > 10 minutes occurs
User Problem Resolution	Best effort	4 hour response 24 hour resolution
User Support communication	Web Site E-mail	Web Site E-mail Phone (12 hour work day)
Admin Problem Resolution	4 hour response 24 hour response	1 hour response 8 hour resolution
Admin Support communication	Web Site E-Mail	Web Site E-Mail Phone (24x7)
User self-management	None	Auditor role – identified customers can view the SDP SysAdmin GUI
Reports	**Security** Past month #/ratio of failed SPAs and failed User Authentication attempts (if relevant) Past month #/ratio dropped packets (CNTL, GW) **SLA Report** Service outage time (minutes/month) Admin Problem Resolution KPIs **Usage** Total BW Transferred (per month)	**Security** #/ratio of failed SPAs and failed User Authentication attempts (if relevant) – history and trend; geolocation #/ratio dropped packets (CNTL, GW) – history and trend; geolocation Monthly Security Assessment Report - Protected Service “blackness” grade - Server encryption testing **SLA Report** Service outage time (minutes/month) Admin Problem Resolution KPIs Customer Problem resolution KPIs **Usage** Total BW Transferred weekly; history and trend. Per user connection audit reports; time connected; total bytes transferred

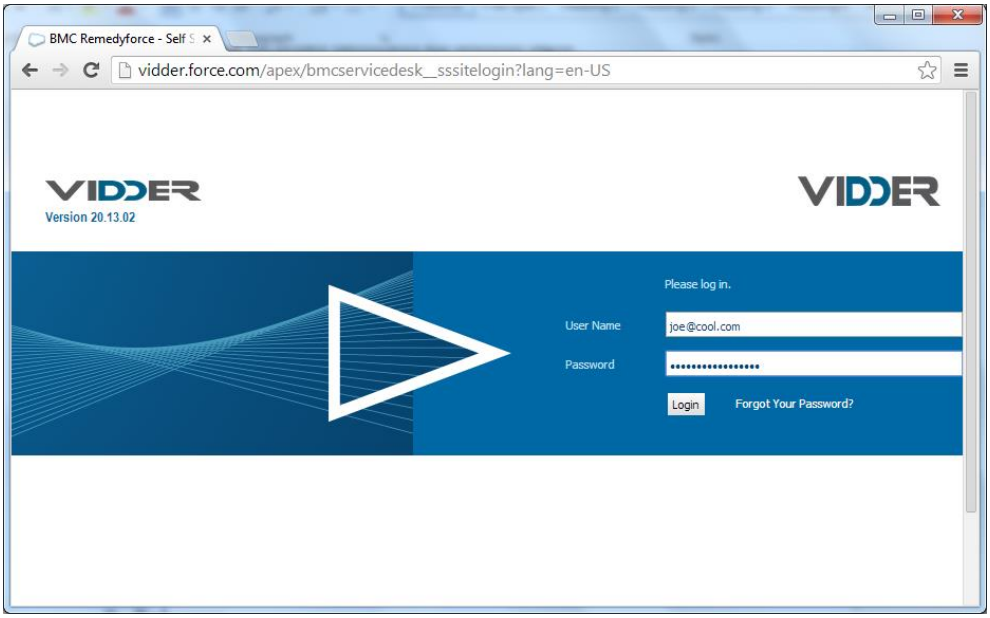
Customer Support

Email Support

Customers can use service@vidder.com to initiate incident reports or service requests if they prefer to use email as the reporting mechanism. Sending an email to this address automatically generates an incident ticket in Remedyforce if originating from an address that is already configured. Regardless, the email message is delivered to the Service Operations Team to respond.

Online Support

Customers can use https://vidder.force.com to initiate incident reports or service requests if they prefer to use a web form as the reporting mechanism. A customer will have the option to report an incident or open a service request.



Once an incident or service request is generated, an email is automatically sent to both the originator and all Tier 1 support engineers. Incident Identification and Resolution begins for incidents.

Phone Support

Under Enterprise support contracts, support calls will be supported via a toll-free line that is provided to all customers. Once a support case is opened, the support engineer will provide the caller with his or her direct extension for future calls on this specific incident or service request. If no Level 1 support engineer is available for ten seconds, the Nextiva system will escalate the call to Level 2.

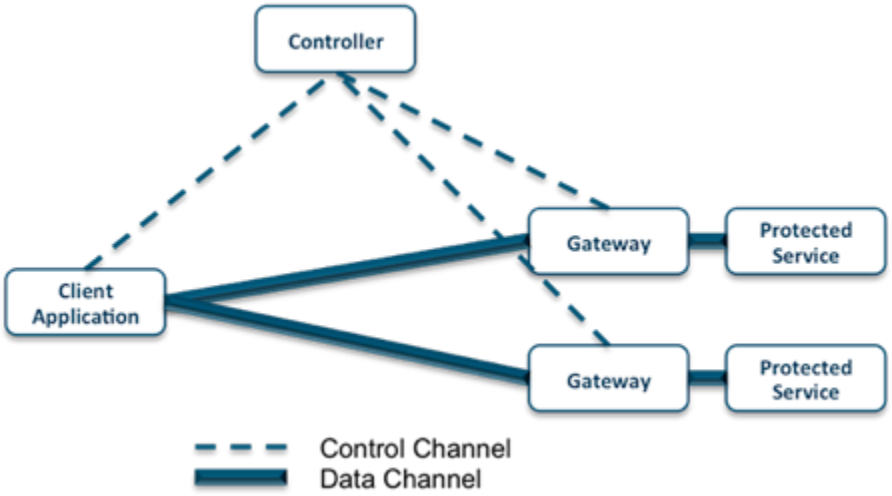
Appendix: SDP High Level Functional Description

SDP Architecture

The Software Defined Perimeter (SDP) is a new approach to security that creates dynamically provisioned, "air-gapped networks" anywhere in the world. An air-gapped network is one that is completely isolated from all unsecured networks, and which, therefore, mitigates network-based attacks.

The Software Defined Perimeter (SDP) is composed of three components: the Controller, the App, and the Gateway.

SDP Architecture



The **Controller** is the intelligent gatekeeper to the Software Defined Perimeter. It uses a military-grade, top secret command and control channel to securely communicate with the other components of the system via out-of-band, encrypted communications. The Controller enables these key functions of a top secret network:

- Device appraisal and user authentication prior to providing network connectivity to eliminate all unauthorized network paths to protected services. *It's hard to attack what you can't see*.
- Dynamic provisioning of all endpoint connectivity and cryptographic algorithms to create a need-to-know network.
- Obfuscation of the Controller from unauthorized devices to mitigate denial of service (DoS) attacks and many other types of attacks on the Controller.
- Real-time control over the overall system topology to react to changing networking environments and maintain a high level of availability and performance.

The **App** is the fortified entrance to the Software Defined Perimeter. It facilitates device and user authentication to the Controller and receives instructions from the Controller on how to create encrypted connections to the authorized Gateways. The App enables these key functions of a top secret network:

- A cryptographically secure communication channel to connect to an obfuscated Controller such that all connections from unauthenticated devices are rejected.
- Derivation and communication of device and user authentication to the Controller over encrypted tunnels to ensure that only authorized devices and users receive access.
- Secure storage of cryptographic material such that compromising the private key is very, very difficult.
- Dynamically generated, mutually authenticated, short-lived, encrypted tunnels to authorized services that are cryptographically secure from unauthorized users.

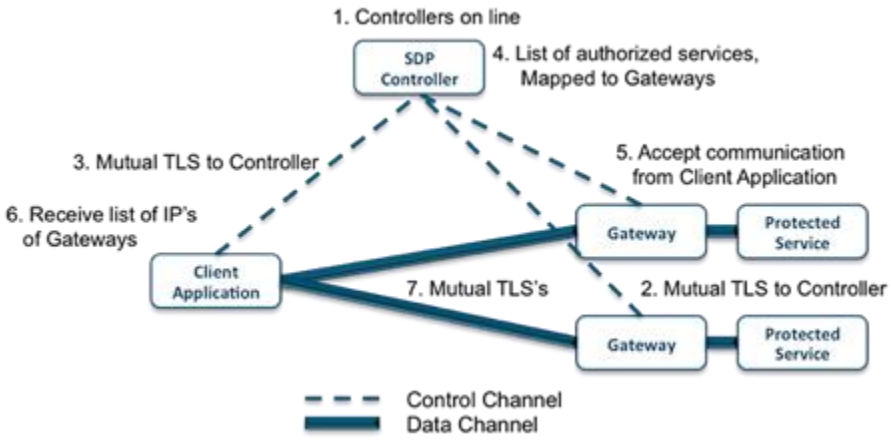
The **Gateway** is the impenetrable wall surrounding the protected Internet-facing application—an impenetrable wall that can only be accessed from the App after being authorized by the Controller. The Gateway enables these key functions of a top secret network:

- The complete rejection of connections to the Internet-facing applications from all unauthorized devices and users to mitigate all types of DoS attacks.
- The complete obfuscation of Internet-facing applications from all unauthorized devices and users to mitigate the OWASP Top 10 vulnerabilities and man-in-the-middle attacks.
- Communication from the user's device to the Internet-facing application over port 443 for all underlying protocols to enable fat client applications to obtain the ubiquity of reach of the Internet.

SDP Workflow

The Software Defined Perimeter replicates the control model used in classified, military-grade, top secret networks but with a focus on cloud applications and consumer devices. The Software Defined Perimeter (SDP) is composed of three components: the Controller, the App, and the Gateway.

SDP Architecture



The SDP framework has the following workflow.

1. One or more SDP Controllers are brought online and connect to their optional authentication and authorization services (e.g., PKI, device fingerprinting, geolocation, SAML, OpenID, OAuth, LDAP, Kerberos, multifactor authentication, and other such services).
2. One or more Gateways are brought online. These Gateways connect to, and authenticate to, the Controllers. However, they do not acknowledge communication from any other hosts and will not respond to any non-provisioned request.
3. Each App that is brought on line connects with, and authenticates to, the SDP Controllers.
4. After the App authenticates to the SDP Controller, the SDP Controller determines a list of services to which the App is authorized to communicate, and to the Gateways that connect to them.
5. The SDP Controller instructs the Gateways to accept communication from the Apps, as well as, defining any optional policies required for encrypted communications.
6. The SDP Controller gives the Apps the list of Gateways it is authorized to communicate with, as well as, defining any optional policies required for encrypted communications.
7. The Apps initiates a mutual VPN connection to each authorized Gateway.