Software Defined Perimeter Working Group

SDP Hackathon Whitepaper

April 2014

© 2014 Cloud Security Alliance – All Rights Reserved.

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance SDP Hackathon Whitepaper at http://www.cloudsecurityalliance.org, subject to the following: (a) the Document may be used solely for your personal, informational, non-commercial use; (b) the Document may not be modified or altered in any way; (c) the Document may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Document as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Software Defined Perimeter Hackathon Whitepaper (2014).

Executive Summary

In 2013, Cloud Security Alliance (CSA) launched the Software Defined Perimeter Initiative, a project designed to develop an architecture for creating highly secure and trusted end-to-end networks between any IP addressable entities, allowing for systems that are highly resilient to network attacks.

In February 2014, CSA sponsored the *Software Defined Perimeter Hackathon*, an event challenging hackers to attack a server defended by a software defined perimeter (SDP). The SDP is a new approach to security that mitigates network-based attacks by creating dynamically provisioned perimeters for clouds, demilitarized zones, and data center infrastructures. The first person to successfully penetrate the server would be awarded an all-expenses paid trip to Black Hat and DEFCON, but while more than 10 billion packets were fired at the SDP from around the world, no attacker broke through even the first of five layers of security controls specified by the SDP architecture.

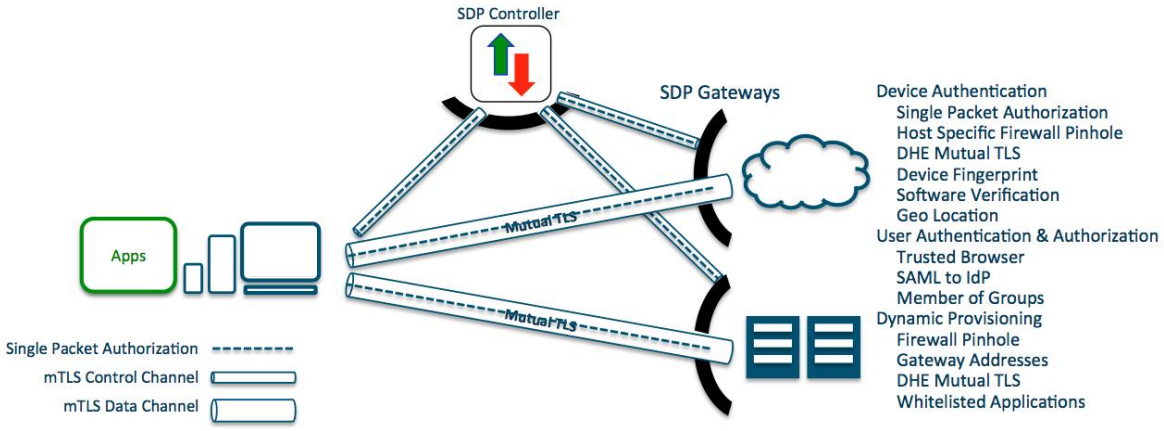
This paper provides a detailed explanation of SDP, its multiple layers of security controls, and the results of the hacking contest.

© 2014 Cloud Security Alliance - All Rights Reserved.

Software Defined Perimeter

The software defined perimeter (SDP) is a new approach to security that mitigates network-based attacks by creating dynamically provisioned perimeters anywhere in the world, including clouds, demilitarized zones (DMZs), and data centers.

The traditional networking model provides visibility and connectivity within the network and then adds a number of point controls to prevent access from untrusted systems. SDP provides zero visibility and zero connectivity, only establishing connectivity after end points prove they can be trusted. This approach prevents essentially all network-based attacks.



Five Layers of Security Controls

The software defined perimeter architecture consists of five layers of security controls: single packet authorization, mutual transport layer security, device validation, dynamic firewalls, and application binding. Together, these protocols make it very difficult for attackers to access protected applications.

Single Packet Authorization (SPA)

One of the primary objectives of the software defined perimeter is to make the application infrastructure effectively “black,” or undetectable, showing no domain name system (DNS) information or IP addresses.

Single packet authorization (SPA) enables the software defined perimeter to reject all traffic to it from unauthorized devices. It requires that the first packet to the controller cryptographically verifies that it is an authorized device before being considered for access to the protected service. If visibility is granted, SPA is utilized again to enable the gateway to identify the traffic coming from authorized users and reject all other traffic.

© 2014 Cloud Security Alliance - All Rights Reserved.

Mutual Transport Layer Security (mTLS)

Transport layer security (TLS), also known as secure sockets layer (SSL), was designed to provide device authentication prior to enabling confidential communication over the Internet. The standard was originally designed to provide mutual device authentication. However, in practice, TLS is typically only used to authenticate servers to clients, not clients to servers. The software defined perimeter uses the full TLS standard to provide mutual, two-way cryptographic authentications.

Device Validation (DV)

Mutual TLS proves that the device requesting access to the software defined perimeter possesses a private key that has not expired and that has not been revoked, but it does not prove that the key has not been stolen. Device validation proves that the key is held by the proper device. In addition, device validation attests to the fact that the device is running trusted software and is being used by the appropriate user.

Dynamic Firewalls

Most people are familiar with traditional firewalls that use static configurations to limit incoming and outgoing traffic based on the address information in the IP packet (that is, based on the quintuplet of protocol, source IP address and port, and destination IP address and port). Most enterprise firewalls have ten, hundreds, or even thousands of firewall rules.

Unlike traditional firewalls, dynamic firewalls have only one firewall rule: deny all. Communication with each device is individually enabled by dynamically inserting “Permit <IP quintuplet>” into the firewall policy. In the software defined perimeter architecture, gateways incorporate this dynamic firewall security control.

More specifically, the software defined perimeter dynamically binds users to devices, and then dynamically enables those users to access protected resources by dynamically creating and removing firewall rules in the SDP gateways.

Application Binding (AppB)

After authenticating and authorizing both the device and the user, the software defined perimeter creates encrypted TLS tunnels to the protected applications. Application binding constrains authorized applications so they can only communicate through those encrypted tunnels, and, simultaneously, blocks all other applications from using those tunnels.

© 2014 Cloud Security Alliance - All Rights Reserved.

Hackathon Setup

Attackers signed up for the hackathon anonymously and were then given full access to a reference SDP, including the ability to connect to the reference SDP controller and access servers protected by the SDP gateways. Attackers were also given insider knowledge of the target SDP, including the IP addresses of all components of the infrastructure and a full packet capture of an authorized user connecting to the target SDP and accessing the target server. The attackers' objective was to retrieve a file from a known location on the target server.

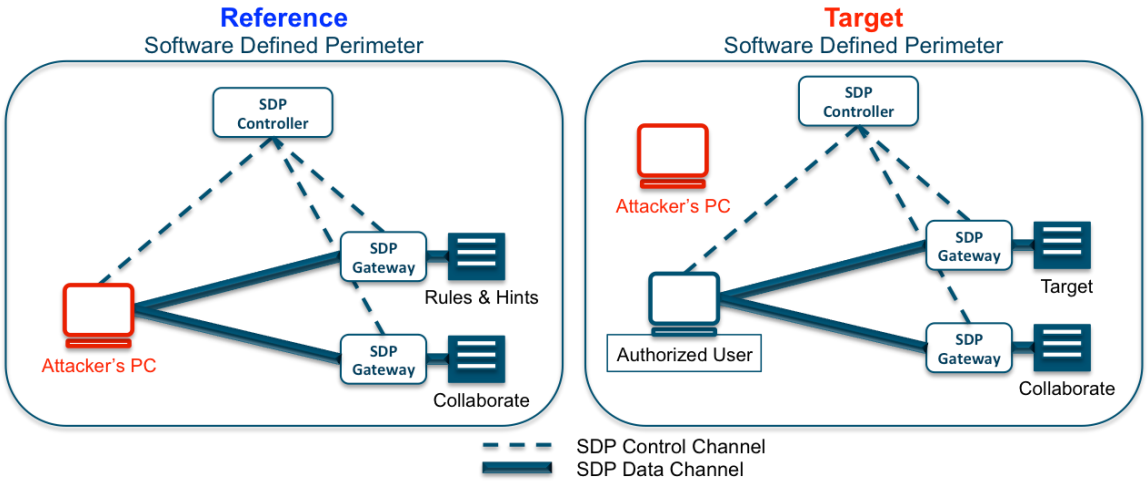


Figure 1. Attackers were provided the IP addresses of all components of the infrastructure and a full packet capture of an authorized user connecting to the target SDP and accessing the target server.

Hackathon Activity and Results

Hackers from all over the world participated in the hackathon. Notable entrants signed on from Argentina, Brazil, Chile, China, Hong Kong, Hungary, Korea, Romania, Russia, UK, and the USA. During the five-day event, over 10 billion packets were fired at the software defined perimeter. However, no one was able to circumvent even the first of the five SDP security controls layers, the single packet authorization protocol.

While these results do not prove that the software defined perimeter architecture can withstand directed attacks from foreign governments, it does validate the robustness and scalability of the software defined perimeter in a real world hackathon. Through its use of well-tested algorithms and multiple levels of security controls wrapped in an easy-to-use workflow, the software defined perimeter provides the highest level of security for the least amount of user effort.

© 2014 Cloud Security Alliance - All Rights Reserved.

Getting Involved with the Software Defined Perimeter Initiative

CSA has several activities and new deliverables planned for SDP. This includes technical specifications, use cases, sample implementations and more hacking contests. We encourage the community to get involved in the continued development of SDP.

To learn more about the software defined perimeter and volunteer opportunities, please visit our website at: https://cloudsecurityalliance.org/research/sdp/

© 2014 Cloud Security Alliance - All Rights Reserved.