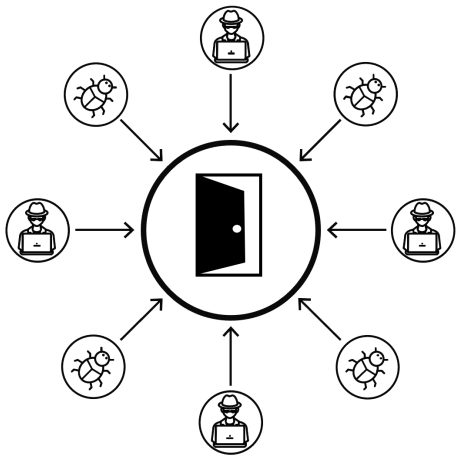
appgate

APPGATE SDP
UNDERSTANDING SINGLE PACKET AUTHORIZATION (SPA)

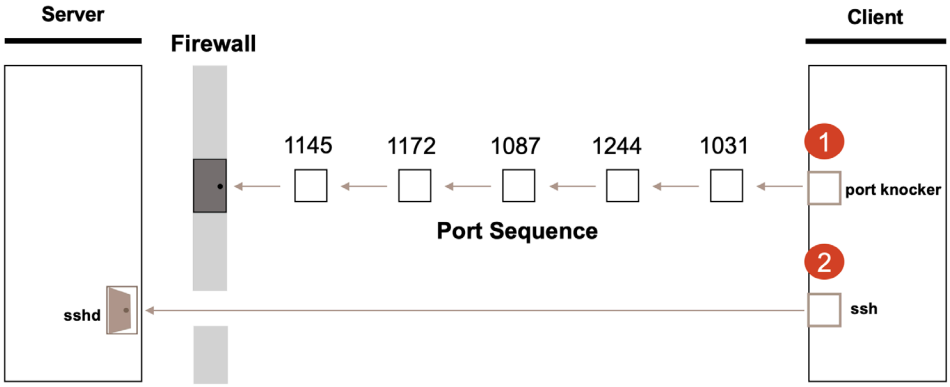
ZERO TRUST NETWORK ACCESS **WHITEPAPER**

Introduction

The network is where key enterprise assets live and has evolved into a decentralized, distributed and increasingly complex and vulnerable environment. This makes it more challenging than ever to secure an expanding attack surface and user-to-resource and resource-to-resource connections. Many legacy security methods are no longer adequate, leaving the door wide open for attackers.



One example is port knocking, which is a predecessor to single packet authorization (SPA). It is a mechanism that externally opens ports on a firewall by creating a connection attempt on a set of closed ports. Once an authorized sequence of connection attempts is received, the firewall rules are dynamically modified and the sending host is permitted to connect over specific ports.



Firewall is opened in response to a specific port sequence

But port knocking is totally dependent on the robustness of the port knocking daemon. If the daemon fails, access will be denied for all users and this enables a single point of failure. A process-monitoring daemon must then be utilized to restart a failed or stalled port knocking daemon process.

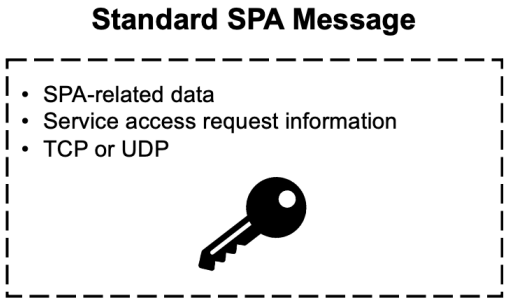
Another challenge with port knocking occurs when it is utilized without cryptographic hashes. This can leave networks vulnerable to IP address spoofing/denial-of-service (DoS) attacks.

In addition, networks with high latency may have issues with port knocking as it relies on packets arriving in a correct sequence. The timing may not align with the transmission control protocol (TCP) assembling of out-of-order packets into that correct sequence. This means that the client may have to resend the correct sequence until it is eventually recognized by the server.

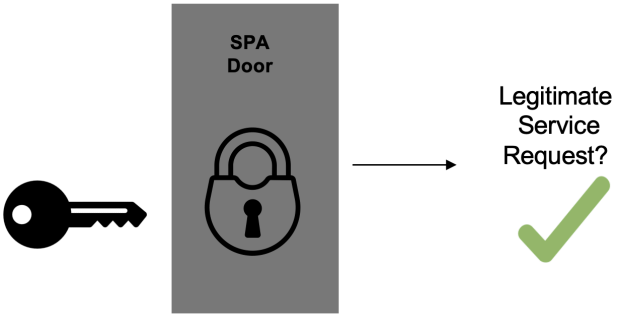
SPA, which uses a single secret knock and does not rely on a sequence for authorization, was created to eliminate many of the inherent vulnerabilities associated with port knocking. SPA hides exposed protocol ports from threat operator reconnaissance behind a "protective door" that can only be opened with authorized keys and tokens.

How SPA Works

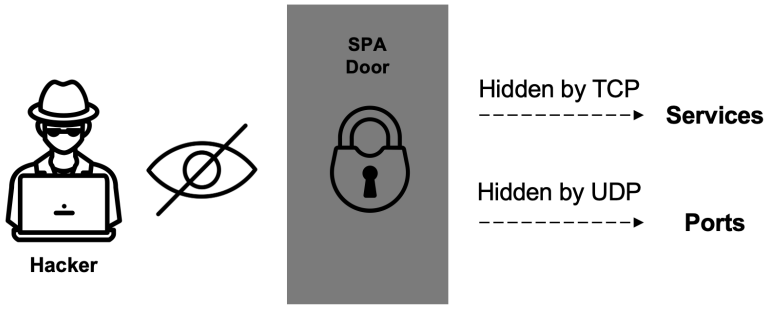
- A device or user can unlock the protective door and interact with specific destination resources only after authorizing with SPA.
- The fundamental premise of SPA is that all connections to port 443 require a unique and cryptographically secured message be sent to the respective destination to communicate with it. This message can be sent with either of the Layer 4 (L4) protocols, TCP or UDP. In addition to the SPA-related data, the message includes information about the service that the connection wants to access.



- The critical factor is that the authorization message is encrypted with a symmetric 256-bit key, known only by the sender and the specific destination. As a result, the appliance can decrypt the message and verify that the access request for the service is legitimate.



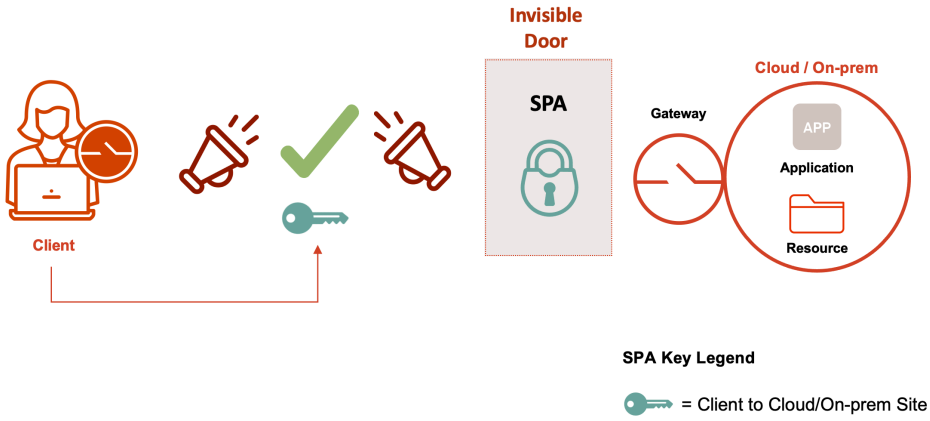
- SPA adds an important additional layer of security. For example, without SPA, anyone can see that port 443 is open and that it accepts "TLS ClientHello" messages. Therefore, the attacker could find the port and try to exploit some known or zero-day vulnerability of OpenSSL to compromise the system. With SPA-TCP, the attacker has no idea that there is such a service and with SPA-UDP, they can't even see that any port is open. Each protocol option has advantages and desirable capabilities.



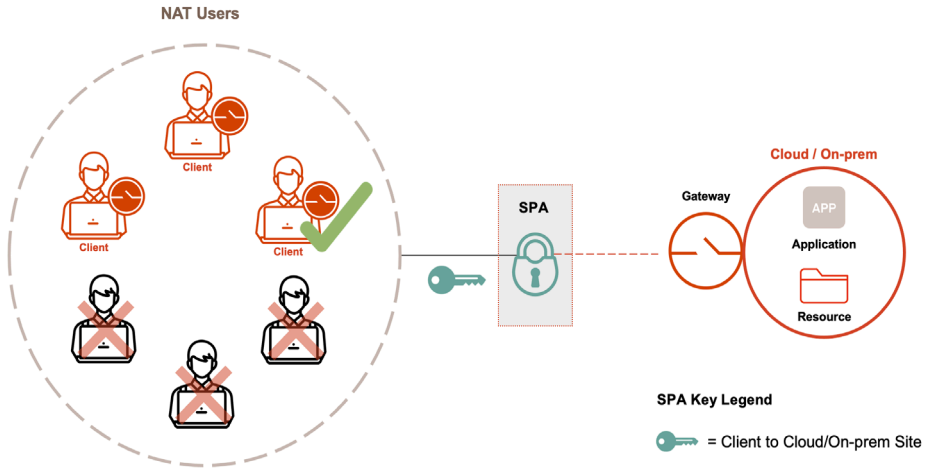
How Appgate SDP Improves the SPA Standard

Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, takes SPA to a whole new level with a unique implementation that includes several key differentiating benefits over others. Appgate SDP has a proprietary TCP/UDP SPA mechanism that leverages the best of both protocol options and can approve who on the network is able to see the door to your important assets.

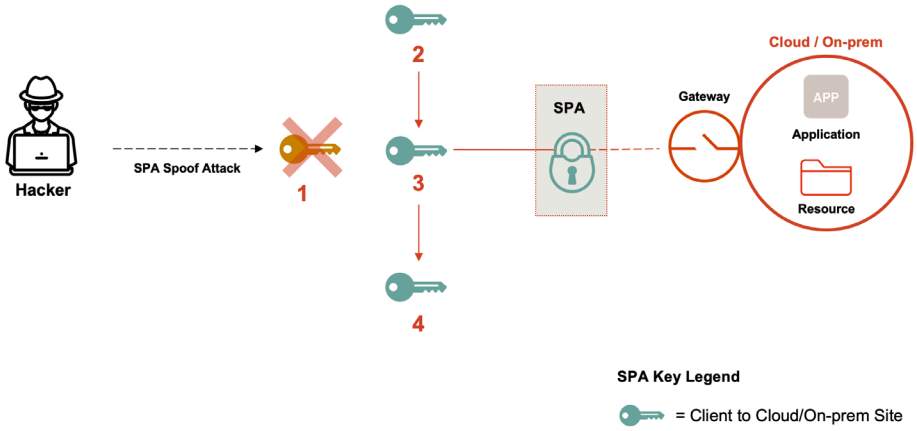
1. **Full verification of authorization.** When a supposedly valid SPA source or client requests access from an Appgate SDP appliance, it will not respond with service or protocol port information unless the sender is verified as a trusted and authorized source. Without the necessary key verification, the appliances and the critical resources they protect are completely cloaked from prying eyes.



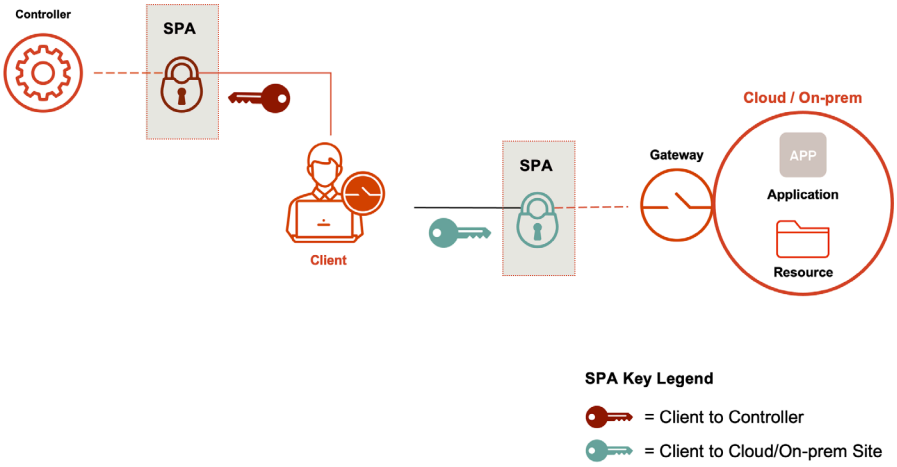
2. **Added user protection behind network address translation (NAT) gateways.** Most SPA implementations are limited because there is no differentiation amongst devices behind a NAT Gateway. In other words, if one user sitting behind a NAT can provide the necessary access keys to open the door to the desired destination, then others can piggyback on that and also be let in, thus compromising the system. Appgate SDP's SPA implementation recognizes and only allows individual users access from a NAT'd network based on individually verified authorization keys and tokens.



3. **Spoof protection (revolving key assignment).** Another important benefit of the Appgate SDP SPA approach over a typical SPA implementation is the fact that it does not leverage static keys for authorization requests. With static keys, a bad actor can spoof a SPA packet and gain access to the critical resource in question. The SPA implementation within Appgate SDP uses a revolving key, which means that within seconds a new key has been generated and a spoofed SPA packet is denied access because the key being spoofed is obsolete.

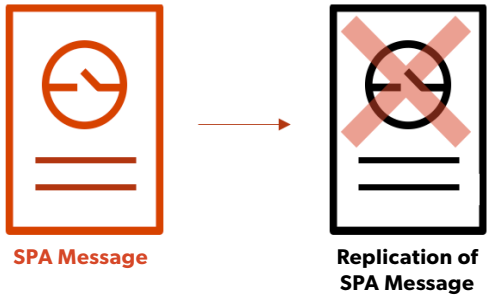


4. **Isolated key distribution.** Appgate SDP also employs an overall protective key distribution system, which utilizes specific keys for each interaction. There are keys used for clients to interact with controllers, and these keys are unique from those used to communicate with the gateways within a given site. Likewise, the inter-appliance interactions between Controllers, Gateways and other appliances are protected with unique SPA keys.

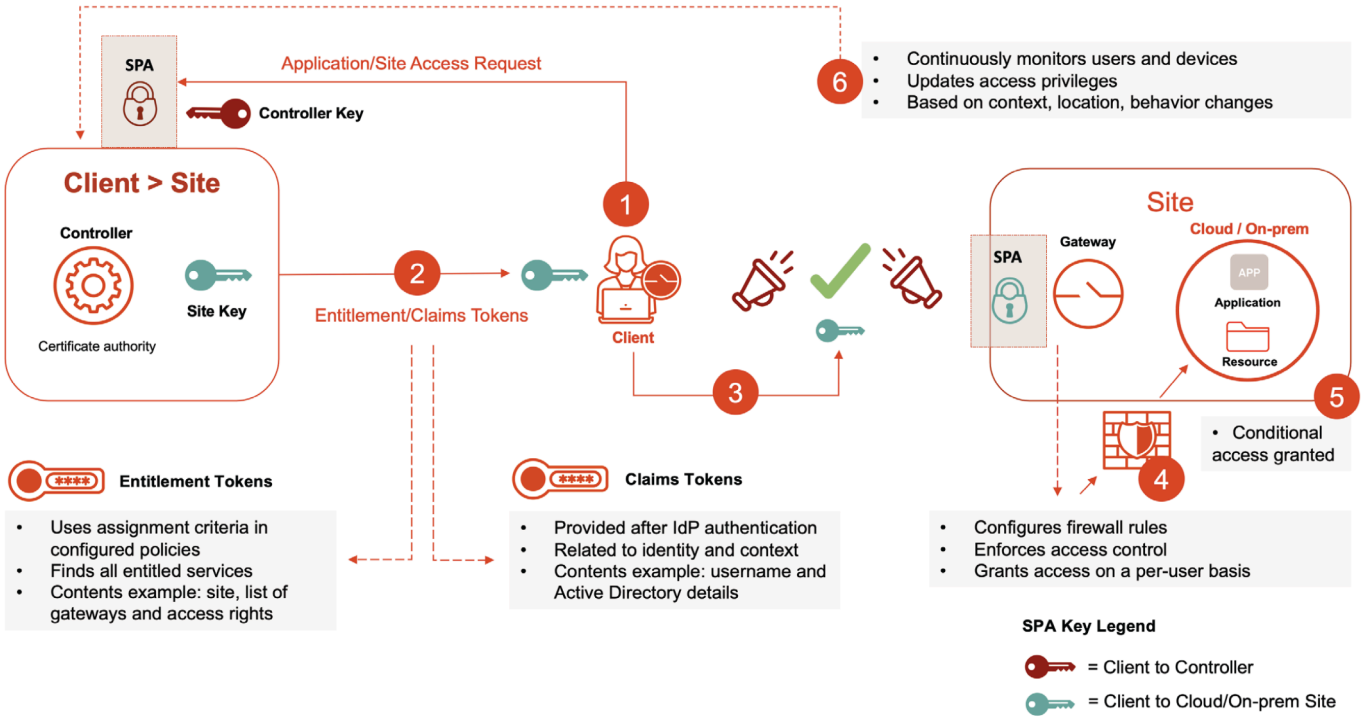


5. **Ensured SPA delivery.** One issue in early versions of SPA was that corporate firewalls could end up dropping SPA messages (TCP or UDP) because firewall engines were not recognizing them. More recent releases of Appgate SDP overcome this by encapsulating the SPA messages inside other known Layer 5 protocols so that the firewalls will allow it.

6. **Replication protection.** Each Appgate SPA message is also crafted in a special way so that malicious users cannot recreate it, replay it or do any other action that would compromise each authorization interaction.



Appgate SDP Client > Resource/Application



About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.

appgate