AppGate SDP and NIST 800-207

Michael Friedrich
Vice President – Cyxtera Federal Group

Cyxtera™

How Does Your Technology Map To NIST 800-207 Key Tenets & Components Mapping

Key Tenets (pages 4&5)

- **All data sources and computing services are considered resources**
  - ✓ AppGate SDP works at OSI layers 3,4 and some URL filtering at layer 7. Further, it works across all three major public clouds, major OS's (mobile and non-mobile) and hypervisors. This allows a single solution to protect data sources and computing services wherever they are and on whatever device is in use, defined by the policies associated with the individual and their device(s)
- **All communication is secure regardless of network location**
  - ✓ AppGate SDP leverages mTLS FIPS 140-2 compliant and 3rd party validated encryption on every connection to an authorized workload by a user leveraging an approved and validated complied to connect device (i.e. positive control) – regardless of the user's location. That is, even on-premises users traffic is encrypted.
- **Access to individual enterprise resources is granted on a per-connection basis**
  - ✓ AppGate SDP leverages a policy engine based on the user and device attributes (defined and learned in the authorization process) to grant granular access down to the IP, port and protocol. This access is micro-segmented to just that user's needed and required access at that point in time (if permissible)
- **Access to resources is determined by policy, including the observable state of user identity and the requesting system, and may include other behavioral attributes**
  - ✓ AppGate SDP inherently leverages least privilege access. All access is granted based on defined policies that validate numerous and varied conditions. Further, the platform is based on REST API's allowing for seamless integration with other tools to help create a behavioral user profile for continued and dynamic access control

How Does Your Technology Map To NIST 800-207 Key Tenets & Components Mapping

Key Tenets (pages 4&5)

- **The enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible**
  - ✓ AppGate SDP has the capability to work both North-South and East-West. By leveraging our Rest API, SAML and scripting capabilities for integration, AppGate SDP is able to create live entitlements to continually monitor for health and security of the associated systems and devices. Any system with the AppGate SDP agent installed can have its configuration (posture) evaluated against access policies, and reported on. This includes server resources.
- **User authentication is dynamic and strictly enforced before access is allowed**
  - ✓ AppGate SDP works with every major MFA authorization vendor that leverages REST API, SAML or scripting capabilities, and supports the ability to enforce step-up authentication based on context. All access via AppGate SDP is considered temporary. AppGate SDP views all access as implicitly denied unless by policy it is permitted (based on the conditions of approval and entitled activities within the policy). By integrating with other vendors solution leveraging API's, tagging, SAML and scripting, we are able to in near-real time, dynamically control and change access on a just in time (JIT) basis. AppGate SDP will not acknowledge access requests that are not defined/permissible at that point in time in the users policy.

How Does Your Technology Map To NIST 800-207 Key Tenets & Components Mapping

Key Components (Pages 7&8)

- **Policy Engine (PE)**
  - ✓ The AppGate SDP controller (virtual or physical) appliance plays the role defined for as the policy engine. Through the AppGate SDP controller clients are able to create policies, create trusted access, define blacklists, etc. It is through the comply to connect process that AppGate SDP enforces the positive control of the policy engine
- **Policy Administrator (PA)**
  - ✓ The AppGate SDP controller acts as both the PE and PA. The PA role of creating the token to grant access through the PEP is the end result of the comply to connect (positive control) process completed through the AppGate SDP controller
- **Policy Enforcement Point (PEP)**
  - ✓ The AppGate SDP Gateway (virtual or physical) acts as the PEP. A clients' token (along with the individual mTLS client sessions) are terminated onto the PEP. The PEP then enforces micro-segmentation and logging. The actions permitted on the PEP are contained in the signed token sent to the PEP from the PE/PA process within the AppGate SDP Controller
- **Continuous Diagnostics and Mitigation (CDM) System(s)**
  - ✓ The AppGate SDP system provides continuous status on the health of the AppGate system via dashboards and are available to extract to automation tools for updating as needed
- **Industry Compliance System**
  - ✓ AppGate SDP is Common Criteria (CC) certified up to EAL 2+. The + is for network and firewall devices as defined in the protection profiles. There is currently no protection profile defined for a Software Defined Perimeter. AppGate SDP's CC certificate and target of evaluation (TOE) documentation is available on the CC site (https://commoncriteriaportal.org/products/). Included the evaluation process for CC was the cryptography (FIPS 140-2), Lifecycle support, security management, identification and authentication and user data protection

How Does Your Technology Map To NIST 800-207 Key Tenets & Components Mapping

Key Components (Pages 7&8)

- **Threat Intelligence Feed(s)**
  - ✓ AppGate SDP accepts inputs (i.e. threat feeds) via REST API, SAML or scripted integration. These feeds of information can be integrated into policies to create automated access controls/playbooks. If a feed from an outside source comes into AppGate SDP and there is a policy set to create an action, AppGate SDP will automatically implement the actions dictated in the policy
- **Data Access Policies**
  - ✓ AppGate SDP works primarily at OSI layers 3&4 (with some layer 7 URL filtering also available). AppGate SDP will manage the access from a network perspective to the resources where the data is being hosted/created. The data access policies are created within the AppGate PE/PA process as defined in the AppGate SDP Controller. Policies are created and managed via the AppGate SDP Controller. The policies can account for role, device, location, time, patch level and much, much more
- **Enterprise Public Key Infrastructure (PKI)**
  - ✓ AppGate SDP has the ability to leverage enterprise certificates in the mTLS process and further generates a certificate of its own. In addition, it can makes calls to federal PKI services such as the federal bridge to validate CAC/PIV badges in the authentication process to access a workload(s). Further, AppGate SDP is compliant with the derived credentials directive from OMB as clients are fully able to leverage locally loaded enterprise certificates to be used in the access control process
- **ID Management System**
  - ✓ AppGate SDP comes with several options when it comes to identity management. AppGate SDP does have a local DB option, but also can integrate with AD, LDAP, SAML (Federal Bridge - CAC/PIV) or Radius based ID systems. Through this process, AppGate SDP retrieves the roles and attributes applicable to that user and device at that point in time, complete the comply to connect process and create the micro-segmented access

How Does Your Technology Map To NIST 800-207 Key Tenets & Components Mapping

Key Components (Pages 7&8)

- **Security Incident and Event Management (SIEM) System**
  - ✓ AppGate SDP gathers logs on attempted and completed sign in's to AppGate SDP. Further, it logs each users attempted and completed actions (i.e. accessing a host/workload). The logs AppGate SDP gathers include everything set up to be learned or authenticated about the user and device(s) in the comply to connect process. This would include all devices, location, time, IP, MAC ID, patch levels and much, much more. All of this information is available locally with a provided ELK stack capability, but can be further extracted to all major SIEM services. Further, as long as that SIEM service has an API Appgate SDP can interact with, much like other sources of information/feeds, AppGate SDP can interact (push or pull) with the SIEM to enforce policies for access controls
- **Industry Compliance Systems**
  - ✓ AppGate SDP can perform device profile/posture checks, and be used to validate devices against organizational configuration compliance. AppGate SDP can use a device's compliance as an attribute in an access policy, and therefore control user access based on compliance.

Sample Use Cases Addressed by AppGate SDP

- Remote Worker – VPN replacement
- Enabling digital transformation – positive control across multiple operating environments enabling higher and more secure productivity
- Microsoft Office 365 Access Control
- Low probability of observation (LPO) and low probability intercept (LPI)
- Remove lateral movement
- Secure High Value Assets
- Micro-segmentation concerning foreign nationals and 3rd party risks
- Securing virtual desktop infrastructure (VDI) and centralized operations
- Securing the cloud
  - Containers
  - Storage
  - Access
- Making bring your own device secure/comply to connect
- Enabling DevOps
- Cloud Migration

Technical Challenges Experienced or Discovered Along The Way To Help Agencies Down The Zero Trust Path

- Identity management & role based access control (RBAC) – a clear understanding of who their users are, where they should be accessing what and on what devices, under what conditions
- Network mapping/understanding where and what their data points look like
- Learning to think about the user and the device versus the typical IP SEC VPN policy issue
- Moving from VPN rules based on large networks to modern SDP rules around the user and device(s)
- API, SAML or scripting Integration – helping agencies un-silo their cyber tools to ensure they get smarter integrated tools, not just another tool
- Orchestration of transition from legacy tools to modern integrated tools enabling zero trust

What Standards Are Needed, If Any, In The Zero Trust Space?

- Great job on SP 800-207
- Zero Trust deployments must leverage existing standards (de facto and official)
  - SAML, LDAP
  - REST for inter-system integrations
- Potential Future Standards Areas
  - Other Identity/Authentication Models (e.g. OpenID Connect) ?
  - Standardized Policy Model

www.cyxtera.com