AEP Networks – Product Family Descriptions and Applications

# Series A

Series A is a Secure Application Access gateway that provides a high level of security for organisations who want to allow authorised employees to connect to corporate applications from any network and with any device. Companies can, for example, allow access from home PCs or tablet computers such as iPad and Android devices connected via pubic wireless hotspots without compromising the security of information held in their datacentres.

This secure any-to-any support is provided through the integration of industry-based standard authentication and access methods as well as device fingerprinting to ensure that endpoints meet the minimum security standards required for patch levels, antivirus updates and personal firewalls. Connection to the corporate network is only permitted once these have both been verified.

Series A technology can be provided as a dedicated hardware appliance or as a virtual appliance to provide flexible deployment scenarios. Series A is can be bought using four different licencing models which have been specifically designed for different customer usage scenarios:

|  |  |  |
| --- | --- | --- |
| Licence model | Description | Typical uses |
| Netilla | A secure, remote application access gateway that combines different security methods such as several authentication methods and the creation of V-Realms which allow only selected groups to access certain business applications. | Enterprises who want to give their users secure access to corporate resources from a wide variety of, often unknown, devices thorough a single, secure gateway. |
| LANProtect | A licence based on the number of users requiring secure access to corporate applications, typically through virtual desktop infrastructures. | Enterprises and government organisations that require a secure virtual desktop environment. |
| ServiceProtect | A flexible licence based on the number of CPUs in the gateway hardware for organisations that have unexpected high demands on their infrastructures due to their business models, for example public-facing cloud providers. | Organisations with public facing cloud infrastructures who see increased demand for their services during peak operating times and therefore require flexible and scalable access gateway technology |
| CloudProtect | A subscription based licence that provides Security-as-a-Service (SECaaS) to deliver highly secure, policy-based application and network access using a model that requires no initial CAPEX outlay. | Mobile and fixed line service providers, Managed Service Providers (MSPs), Cloud Service Providers, Large Enterprise organisations who charge internally for IT provision |

In addition to the Secure Application Access gateway hardware appliance or virtual appliance, there is the option to deploy AEP Networks’ load balancer to allow traffic distribution across multiple gateway instances and the Assurance platform (based on Keyper) which adds an additional layer of security to protect cryptographic keys used to secure LANProtect, CloudProtect and Service Protect.

# Series E

Series E is an enhanced grade network encryption solution that allows organisations to securely transmit business sensitive or confidential data over public and private networks without compromising security. This enhanced grade network encryption solution has been designed to ensure easy deployment and management of government-grade IPSEC-based security. Net CA provides the necessary central management capability which significantly reduces the time required for the initial setup and on-going maintenance tasks such as key change and roll over.

Series E encryptors are certified by the UK Government’s CESG Assisted Products Scheme (CAPS) to Enhanced Grade level and by the Ministry of Defence Infosec Product Co-Operation Group.

Series E technology is supplied as dedicated hardware that can either be deployed in a site-to-site configuration to encrypt traffic between two or more locations (Net 100M and NET 20M platforms) or can be used by remote users to connect securely into their corporate infrastructure from any public network (Net Remote platform). Typical uses of the hardware platforms include:

|  |  |  |
| --- | --- | --- |
| Model | Description | Typical uses |
| Net 100M and Net 20M | Enhanced Grade Network Encryptors to provide end-to-end encryption to ensure sensitive or confidential network communications cannot be intercepted over public networks | Enhanced Grade IPSec-based IP security gateway for government organisations; high assurance IPSec-based IP security gateway for enterprises; service providers wanting to gain secure access into companies to provide network management capabilities |
| Net Remote | A secure personal remote access communications encryptor to ensure secure remote access into corporate infrastructures | Remote workers who need secure access to their corporate infrastructures; remote government agencies such as embassies requiring secure communications; armed forces and emergency services who need constant to communication to headquarters without fear of interception |
| Net CA | The central key management platform for all Series E encryptors, certifies public keys, revokes certificates and signs Certificate Revocation Lists | All organisations who deploy Series E Net and Net Remote products so that they can quickly and effectively deploy and manage encryptors without having to perform on-site changes. |

# Series K

Series K is a Key Security and Management solution that generates and stores high-quality keys to protect the integrity of any key-based security system. The platform generates excellent quality cryptographic keys due to the quality of the random seed used to generate them. Once generated, the keys are stored in purpose build hardware that, unlike others, is not exposed to general-purpose operating system vulnerabilities.

The Series K Key Security and Management system is a secure Hardware Security Module (HSM) that allows the deployment of a high-grade public key infrastructure (PKI). It is certified to FIPS-140-2 level 4 which means that it is tamper-reactive and positively destroys key material if the device hardware is compromised. Series K Key Security and Management solutions are used in many different scenarios where digital integrity needs to be ensured through the use of digital signatures. These include:

|  |  |
| --- | --- |
| Customer type | Description |
| Internet companies | Top level internet domain providers who want to implement Domain Name Security System Extensions (DNSSEC) to protect internet clients from forged DNS data (e.g. DNS cache poisoning). Series K ensures that all DNSSEC answers are digitally signed. |
| Online music/application shops | Organisations who sell music or applications online ensure that they are protecting their intellectual property rights by digitally signing each individual download. |
| Electronic gaming companies | In order to meet strict gaming regulations, the integrity of electronic gaming software, for example computerised slot machines, needs to be ensured. This is done by digitally signing all of the gaming software. |
| Credit card companies | Ensure the integrity of credit card transactions by digitally signing all transactions. |

# Series V

Series V is AEP Networks’ Secure Communications Optimised Packet Engine (SCOPE) platform that enables data and voice communications to be optimised even when sub-optimal networks are all that are available. SCOPE is deployed in conjunction with a variety of low bandwidth bearer technologies including terrestrial, 3G, WLAN, radio and satellite and provides compensating technology to delivery maximum voice and data performance in these conditions.

SCOPE has several security and optimisation technologies including:

* *Voice optimisation* – to ensure that voice gets priority and is not impeded by data traffic sharing the same link
* *Web caching* – to maximise the use of low-bandwidth networks while improving the end-user experience
* *Lowest cost network selection* – to select the most effect and cheapest network from those available in a particular location
* *Encryption* – ensuring that all communications are secure even if a public WLAN network is being used.

In addition to being easy to use, the SCOPE platform contains technology that enables the administrator to manage all configuration tasks remotely. This means that the platform can be sent to a remote location before exact configuration details have been determined. This reduces the initial deployment time for mission-critical deployment s and the on-going maintenance costs by eliminating the need for onsite visits by qualified engineers.

SCOPE is available as an office workgroup solution that supports multiple users who need to set up data, voice and video communications in a remote and often temporary location and as a single user solution for individuals travelling outside the office.

SCOPE can be deployed in a wide variety of scenarios including:

|  |  |
| --- | --- |
| Customer type | Description |
| Maritime | Ship-to-shore communications for crew and passenger voice and data communications; point-of-sale transactions; ability to roam between satellites and land-based mobile communications such as 3G |
| Armed forces | In-theatre communications between the field and HQ to provide reliable and secure communications regardless of the network type available |
| Emergency services | In-vehicle communications to provide mobile voice and data communication with guaranteed performance |
| Banking | Integration of legacy networks into modern IP networks to protect investments as banks do not need to upgrade their entire infrastructure immediately to benefit from modern IP network technologies |
| Enterprise | Provides Internet backup facility in the event of a primary failure which is critical for organisations as they move their critical business applications to cloud-based technologies |