HOJA DE DATOS

ARUBA CLEARPASS POLICY MANAGER

La plataforma de políticas de acceso más avanzada disponible

La plataforma Aruba ClearPass Policy Manager proporciona control de acceso a la red en base a roles y a dispositivos para empleados, contratistas y visitantes a través de cualquier infraestructura alámbrica, inalámbrica y VPN de múltiples proveedores.

Con un motor de política interconstruido basado en contexto, soporte para los protocolos RADIUS y TACACS+, opciones para el perfilado de dispositivos y evaluación de postura completa, integración de dispositivos y acceso a visitantes, ClearPass no tiene paralelo como el pilar de la seguridad de la red en cualquier organización.

Para una cobertura más amplia de seguridad, utilizando firewalls, EMM y otras soluciones existentes, ClearPass Exchange permite protección automatizada en contra de amenazas, así como flujos de trabajo de sistemas de seguridad y de TI de terceros que previamente requerían intervención manual.

Adicionalmente, ClearPass soporta capacidades de autoservicio seguro para conveniencia de los usuarios finales. Los usuarios pueden configurar en forma segura sus propios dispositivos para uso empresarial o para acceso a Internet. Los clientes inalámbricos de Aruba pueden proporcionar el registro de dispositivos habilitados por AirPlay, AirPrint, DLNA y UPnP para compartir.

El resultado es una plataforma de administración de políticas completa y escalable que va más allá de las soluciones AAA tradicionales para entregar capacidades extensas de cumplimiento para los requerimientos de seguridad de dispositivos distribuidos por TI y para BYOD (bring-your-own-device).

CARACTERÍSTICAS CLAVE

- Cumplimiento de acceso a la red basado en roles para redes Wi-Fi, alámbricas y VPN de múltiples proveedores.
- Liderazgo en la industria en desempeño, escalabilidad, alta disponibilidad y balanceo de carga.
- Plantillas intuitivas de configuración de políticas y herramientas que otorgan visibilidad para localización y resolución de fallas.
- Soporta múltiples fuentes de autenticación/autorización (AD, LDAP, SQL dB) dentro de un servicio.
- Integración de dispositivos mediante autoservicio con autoridad de certificados (CA) interconstruida para BYOD.

- Acceso de visitantes con personalización extensa, marcas y aprobaciones basadas en patrocinadores.
- Soporta integración con NAC, Microsoft NAP y EMM/MDM para evaluaciones de dispositivos móviles.
- Integración completa con sistemas de terceros, como SIEM, seguridad de Internet y EMM/MDM.
- Soporte para SSO (Single Sign-On) y Aruba Auto Sign-On vía SAML v2.0.
- Reportes avanzados de todas las autenticaciones de usuarios válidas y fallidas.
- Perfiles interconstruidos utilizando DHCP y TCP fingerprinting.
- Hardware y soporte virtual para dispositivos ESXi y Hyper-V.
- Actualización automática de clusters.
- Motor ingress avanzado para protección en contra de amenazas.
- Descubrimiento de atributos de dispositivos con acceso a la red.

LA DIFERENCIA DE CLEARPASS

ClearPass Policy Manager es la única plataforma de políticas que hace cumplir centralmente todos los aspectos de seguridad de acceso de grado empresarial para cualquier industria. El cumplimiento granular de políticas está basado en el rol, tipo de dispositivo, método de

autenticación, atributos de EMM/MDM, operación correcta de dispositivos, patrones de tráfico, ubicación y horario del día.

ClearPass ofrece soporte extenso a infraestructuras inalámbricas, alámbricas y VPNs de múltiples proveedores, lo cual permite que TI despliegue fácilmente políticas de movilidad seguras en cualquier ambiente.

La escalabilidad de despliegue soporta decenas de miles de dispositivos y autenticaciones, lo cual sobrepasa las capacidades ofrecidas por soluciones AAA legadas. Existen opciones para organizaciones pequeñas a grandes, desde ambientes locales a distribuidos.

GENERACIÓN AVANZADA DE REPORTES Y ALERTAS CON PERSPECTIVA

Policy Manager incluye capacidades avanzadas para generación de reportes vía datos personalizables – autenticaciones, dispositivos perfilados, datos de visitantes, dispositivos integrados y operación correcta de puntos terminales, todo esto en un tablero de control sencillo de visualizar. También incluye capacidades granulares para alertas.

ADMINISTRACIÓN AVANZADA DE POLÍTICAS

Cumplimiento de visibilidad para ambientes alámbricos e inalámbricos Con ClearPass, las organizaciones pueden desplegar redes inalámbricas utilizando cumplimiento 802.1X basado en normas para fuerte

autenticación ClearPass también ofrece una forma de crear políticas que no son .1X en redes alámbricas con OnConnect – para aquellas organizaciones que no estén preparadas para operar completamente con 802.1X y AAA a lo largo de sus infraestructuras alámbricas. ClearPass permite un enfoque híbrido para permitir que TI obtenga perspectivas acerca de todos los dispositivos – computadoras, smartphones e IoT – que estén accediendo a la red.

Se pueden utilizar métodos de autenticación concurrentes para soportar una variedad de casos de uso. También incluye soporte para autenticación multifactorial basada en tiempos de inicio de sesión, verificaciones de postura y otro contexto, como un nuevo usuario, un nuevo dispositivo y más.

Se pueden utilizar atributos de múltiples almacenes de identidad, como Microsoft Active Directory, directorios que cumplan con LDAP, bases de datos SQL que cumplan con ODBC, servidores de tokens y bases de datos internas a través de dominios dentro de una sola política para obtener control muy fino.

Los datos contextuales de estos dispositivos perfilados permiten que TI pueda definir cuáles dispositivos pueden acceder a través de la red alámbrica, VPN, o red inalámbrica.

Se utilizan cambios en los perfiles de dispositivos dinámicamente para modificar privilegios de autorización. Por ejemplo, si una laptop Windows aparece como una impresora, las políticas de ClearPass pueden revocar o negar el acceso automáticamente.

Configuración de dispositivos segura para dispositivos personales ClearPass Onboard proporciona aprovisionamiento automatizado de cualquier dispositivo Windows, Mac OS X, iOS, Android, Chromebook y Ubuntu mediante un portal impulsado por usuarios auto guiado. SSIDs requeridas, parámetros X y certificados de seguridad se configuran automáticamente en dispositivos autorizados.

Administración personalizable de visitantes
ClearPass Guest simplifica los procesos de flujos de trabajo para que los recepcionistas, empleados y otro personal que no sea de TI pueda crear cuentas de visitantes temporales para acceso seguro a Internet mediante Wi-Fi y la red alámbrica. Auto registro, creación de patrocinadores y credenciales en masa soporta cualquier necesidad de acceso a visitantes – enterprise, retail, educación, grandes eventos públicos.

Revisiones de operación correcta de dispositivos
ClearPass OnGuard aprovecha los agentes persistentes y de solubles para efectuar evaluaciones avanzadas de postura de puntos terminales sobre conexiones inalámbricas, alámbricas y VPN. Las capacidades de OnGuard para verificar la operación correcta de dispositivos asegura el cumplimiento y las protecciones de seguridad antes de que los dispositivos se conecten.

CAPACIDADES ADICIONALES DE ADMINISTRACIÓN DE POLÍTICAS

Integración con sistemas de seguridad y flujos de trabajo
La interoperabilidad de ClearPass Exchange incluye APIs basadas en REST y en el reenvío de flujos de datos syslog hacia y desde ClearPass bajo demanda que se pueden utilizar para facilitar flujos de trabajo con MDM, SIEM, PMS de firewalls, call centers, sistemas de admisión y más. El contexto se comparte entre cada componente para cumplimiento y visibilidad de políticas de extremo a extremo.

Conéctese y las apps de trabajo se podrán utilizar
Las capacidades de ClearPass Auto Sign-On facilitan tremendamente el acceso a apps de trabajo en dispositivos móviles. Una autenticación de red válida automáticamente conecta los usuarios a las apps móviles empresariales para que puedan comenzar a trabajar inmediatamente.

El soporte de SSO (Single Sign-On opera con Ping, Okta y otras herramientas de administración de identidades para mejorar la experiencia de los usuarios en aplicaciones basadas en SAML 2.0.

ESPECIFICACIONES

Dispositivos de ClearPass Policy Manager

ClearPass Policy Manager está disponible como hardware o como un dispositivo virtual que soporta 500, 5,000 y 25,000 dispositivos que se estén autenticando. Los dispositivos virtuales se soportan en VMware ESX/i y en Microsoft Hyper-V.

- ESX 4.0, ESXi 4.1, hasta 6.0
- Hyper-V 2012 R2 y Windows 2012 R2 Enterprise

Dentro de un cluster activo, se pueden desplegar dispositivos virtuales, así como dispositivos en hardware, para mejorar la escalabilidad y redundancia.

Platforma

- Servicios AAA interconstruidos – RADIUS, TACACS+ y Kerberos
- Autenticación y autorización Web, 802.1X, que no son 802.1X y RADIUS
- Reportes avanzados, análisis y herramientas de localización y resolución de fallas
- Re direccionamiento de portal cautivo externo a equipo de múltiples proveedores
- Utilería para simulación interactiva de políticas y modo monitor
- Múltiples portales de registro de dispositivos – Guest, Aruba AirGroup, BYOD, dispositivos no administrados
- Plantillas de despliegue para cualquier tipo de red, almacén de identidades y punto terminal
- Seguridad de acceso para Admin/Operador vía certificados CAC y TLS
- Túneles IPsec

Soporte para marcos de trabajo y protocolos

- RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML v2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 y 2, EAP-MD5
- NAC, Microsoft NAP
- Autenticación de máquinas Windows
- MAC auth
- Auditoría (reglas basadas en escaneo de puertos y vulnerabilidad)
- OCSP (Online Certificate Status Protocol)
- SNMP generic MIB, SNMP private MIB
- CEF (Common Event Format), LEEF (Log Event Extended Format)
- TLS 1.2

Almacenes de identidad soportados

- Microsoft Active Directory
- RADIUS
- Cualquier directorio que cumpla con LDAP
- Cualquier servidor SQL que cumpla con ODBC
- Servidores de Tokens
- Almacén SQL integrado, lista de hosts estática
- Kerberos

Normas RFC

- 2246, 2248, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3576, 3579, 3580, 3748, 4017, 4137, 4849, 4851, 5216, 528, 7030

Internet drafts

- EAP Versiones 0 y 1 protegidas, extensiones Microsoft CHAP, aprovisionamiento dinámico utilizando EAP-FAST, TACACS+

Validaciones de aseguramiento de información

- FIPS 140-2 – Certificate #2577

Métodos de perfilado

- DHCP, TCP, MAC OUI, ClearPass Onboard, SNMP, Cisco device sensor

	Dispositivo ClearPass 500 (JW770A*)	Dispositivo ClearPass 5K (JW771A*)	Dispositivo ClearPass 25K (JW772A*)
ESPECIFICACIONES DEL DISPOSITIVO			
Modelo de Hardware	Unicom S-1200 R4	Dell R220 XL	Dell R630 XL
CPU	(1) Eight Core 2.4GHz Atom C2758	(1) Quad Core Xeon 3.4 GHz E3-1231_V3	(2) Six Core Xeon 2.4GHz E5-2620_V3
Memoria	8 GB	8 GB	64 GB
Almacenamiento en disco duro	(1) disco duro SATA (7.3K RPM) 1TB	(2) discos duros SATA (7.2K RPM) 1TB, controlador RAID-1	(6) discos duros SAS (10K RPM) 600GB Hot-Plug, Controlador RAID-10
Administración Out of Band	N/A	Dell Baseboard Management Controller	Dell iDRAC 8 Enterprise
Puerto Serial	Si (RJ-45)	Si (DB-9)	Si (DB-9)
ESCALABILIDAD DEL DISPOSITIVO			
No. máximo de puntos terminales	500	5,000	25,000
FACTOR DE FORMA			
Dimensiones (WxHxD)	17.2" x 1.7" x 11.3"	17.09" x 1.67" x 15.5"	18.98" x 1.68" x 27.57"
Peso (Config Max)	8.5 Lbs	16.97 Lbs	Hasta 37 Lbs
ALIMENTACIÓN ELÉCTRICA			
Fuente de alimentación	200 watts max	250 watts max	750 watts max
Redundancia de alimentación	N/A	N/A	Opcional
Voltaje de entrada AC	100/240 VAC auto-seleccionable	100/240 VAC auto-seleccionable	100/240 VAC auto-seleccionable
Frecuencia de entrada AC	50/60 Hz auto-seleccionable	50/60 Hz auto-seleccionable	50/60 Hz auto-seleccionable
CARACTERÍSTICAS AMBIENTALES			
Temperatura de operación	5° C a 35° C (41° F a 95° F)	10° C a 35° C (50° F a 95° F)	10° C a 35° C (50° F a 95° F)
Vibración de operación	0.25 G a 5 Hz a 200 Hz por 15 minutos	0.26 G a 5 Hz a 350 Hz por 15 minutos	0.26 G a 5 Hz a 350 Hz por 15 minutos
Shock de operación	1 pulso de shock de 20 G hasta por 2.5 ms	1 pulso de shock de 31 G hasta por 2.6 ms	1 pulso de shock de 40 G hasta por 2.3 ms
Altitud de operación	-16 m a 3,048 m (-50 ft a 10,000 ft)	-16 m a 3,048 m (-50 ft a 10,000 ft)	-16 m a 3,048 m (-50 ft a 10,000 ft)

* El CP-HW-500 es ahora el JW770A, el CP-HW-5K es ahora el JW771A y el CP-HW-25K es ahora el JW772A.

	Dispositivo ClearPass 5K (JX921A)	Dispositivo ClearPass 25K (JX920A)
ESPECIFICACIONES DEL DISPOSITIVO		
Modelo de Hardware	HPE DL20 Gen 9	HPE DL360 Gen 9
CPU	(1) Xeon 3.5Ghz E3-1240v5 with Four Cores (8 Threads)	(2) Xeon 2.4GHz E5-2620_V3 with Six Cores (12 Threads)
Memoria	16 GB	64 GB
Almacenamiento en disco duro	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) SAS (10K RPM) 600GB Hot-Plug hard drives, RAID-10 controller
Administración Out of Band	HPE Integrated Lights-Out (iLO) Standard	HPE Integrated Lights-Out (iLO) Advanced
Puerto Serial	Yes (Virtual Serial via iLO)	Yes (DB-9)
ESCALABILIDAD DEL DISPOSITIVO		
No. máximo de puntos terminales	5,000	25,000
FACTOR DE FORMA		
Dimensiones (WxHxD)	17.11" x 1.70" x 15.05"	17.1" x 1.7" x 27.5"
Peso (Config Max)	Hasta 19.18 Lbs	Hasta 33.3 Lbs
ALIMENTACIÓN ELÉCTRICA		
Fuente de alimentación	HPE 900W AC 240VDC Power Input FIO Module*	HPE 500W Flex Slot Platinum Hot Plug Power Supply
Redundancia de alimentación	Opcional	Opcional
Voltaje de entrada AC	100/240 VAC auto-seleccionable	100/240 VAC auto-seleccionable
Frecuencia de entrada AC	50/60 Hz auto-seleccionable	50/60 Hz auto-seleccionable
CARACTERÍSTICAS AMBIENTALES		
Temperatura de operación	10° a 35°C (50° a 95°F)	10° C a 35° C (50° F a 95° F)
Vibración de operación	Vibración aleatoria a 0.000075 G^2/Hz, 10Hz a 300Hz, (0.15 G's nominal)	Vibración aleatoria a 0.000075 G^2/Hz, 10Hz a 300Hz, (0.15 G's nominal)
Shock de operación	2 G's	2 G's
Altitud de operación	3,050 m (10,000 ft).	3,050 m (10,000 ft)

* La Fuente de Alimentación Redundante HPE 900W soporta100VAC a 240VAC y también soporta 240VDC.

ORIENTACIÓN PARA PEDIDOS

El ordenar el ClearPass Policy Manager involucra los siguientes pasos:

1. Determine el número de puntos terminales/dispositivos autenticados en su ambiente. Adicionalmente, seleccione la funcionalidad opcional, como visitantes por día, dispositivos BYOD que se configuran para uso empresarial y número total de computadoras que requieren verificaciones de operación correcta.
2. Seleccione la plataforma apropiada (virtual o dispositivo de hardware) dimensionada para incluir el número total de dispositivos y visitantes que requerirán autenticación para su implementación.

NOTA: A los dispositivos virtuales, se les deben proporcionar los mismos recursos para que coincidan con las especificaciones de los dispositivos de hardware.

INFORMACIÓN PARA PEDIDOS

Número de Parte	Descripción
Dispositivos de Hardware	
JW770A	Aruba ClearPass 500 Unique Endpoints with 25 Enterprise Licenses V2 HW Appliance
JW771A	Aruba ClearPass 5000 Unique Endpoints with 25 Enterprise Licenses V3 HW Appliance
JW772A	Aruba ClearPass 25000 Unique Endpoints and Inc 25 Enterprise Licenses V3 HW Appliance
JX921A	Aruba ClearPass DL20 5000 Unique Endpoint and 25 Enterprise Licenses Hardware Appliance
JX920A	Aruba ClearPass DL360 25000 Unique Endpoint and 25 Enterprise Licenses Hardware Appliance
Dispositivo Virtual	
JW335AAE	Aruba ClearPass 500 Unique Endpoints with 25 Enterprise Licenses Virtual Appliance E-LTU
JW336AAE	Aruba ClearPass 5000 Unique Endpoints with 25 Enterprise Licenses Virtual Appliance E-LTU
JW337AAE	Aruba ClearPass 25000 Unique Endpoints with 25 Enterprise Licenses Virtual Appliance E-LTU
Fuentes de Alimentación	
JW790A	Aruba AWCP-HW630-PSU 750W Spr Pwr Supply
JX923A	Aruba ClearPass DL20 Spare Power Supply
JX922A	Aruba ClearPass-Airwave DL360 500W Spare Power Supply
Software de aplicación expandible*	
ClearPass Onboard – device configuration and certificate management	
ClearPass OnGuard – endpoint device health	
ClearPass Guest – visitor access management	
Garantía	
Hardware	1 año en partes/mano de obra**
Software	90 días**

* El software de aplicación expandible está disponible en los siguientes incrementos: 100, 500, 1,000, 2,500, 5,000, 10,000, 25,000, 50,000 y 100,000.

** Se extiende con contrato de soporte

a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com