FICHA DE DADOS

GERENCIADOR DE POLÍTICAS CLEARPASS DA ARUBA

A plataforma de política de acesso mais avançada do mercado

O Gerenciador de Políticas ClearPass da Aruba fornece controle de acesso de rede baseado no dispositivo e em função para funcionários, prestadores de serviço e visitantes e qualquer infraestrutura de multivendas VPN, com fio ou sem fio.

Com um mecanismo de políticas integrado com base em contexto, suporte para protocolo TACACAS+, RADIUS, criação de perfis de dispositivos e avaliação de posturas abrangente, opções de acesso para visitante e onboarding (integração), o ClearPass é uma base para segurança de rede empresarial inigualável.

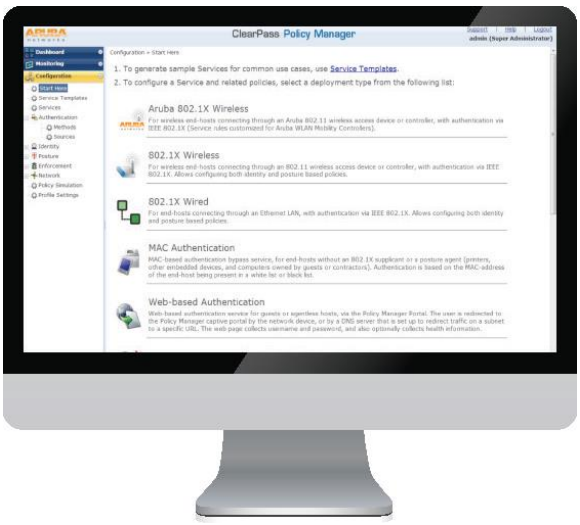
Para maior alcance de segurança, o ClearPass Exchange, por meio do uso de firewalls, EMM e outras soluções existentes, disponibiliza uma proteção automática contra ameaças e realiza o fluxo de trabalho para a segurança de terceira parte e sistemas de TI que, anteriormente, exigiam intervenção manual da equipe de TI.

Além disso, o ClearPass dispõe de funcionalidades de segurança autônomas para conveniência do usuário final. Os usuários podem configurar seus dispositivos para uso empresarial ou acesso a internet de forma segura. Os clientes sem fio Aruba podem realizar o registro de dispositivos habilitados para AirPlay-, AirPrint-, DLNA- e UPnP- para compartilhamento.

O resultado disso é a obtenção de uma plataforma de gerenciamento de políticas escalável e abrangente que vai além das soluções AAA tradicionais para oferecer amplas funcionalidades de reforço para atender às exigências de segurança de ambientes BYOD e administrados por TI.

RECURSOS PRINCIPAIS

- Reforço de acesso à rede baseado em função para redes de multivendas Wi-Fi, VPN e com fio.
- Desempenho líder do setor, escalabilidade, alta disponibilidade e equilíbrio de carga.
- Modelos de configuração de políticas intuitivos e ferramentas de solução de problemas de visibilidade.
- Suporte para múltiplas fontes de autenticação/autorização (AD, LDAP, SQL dB) com um serviço.
- Integração autônoma de dispositivo com certificado de autorização integrado (CA) para BYOD.



- Acesso para visitantes com ampla personalização, desenvolvimento de marca e aprovações baseadas em patrocinadores.
- Suporte para integração NAC e EMM/MDM para avaliações de dispositivo móvel.
- Integração abrangente com sistemas de terceira parte, como SIEM, Internet Security e EMM/MDM.
- Suporte para Single sign-on (SSO) e Aruba Auto Sign-On via SAML v2.0.
- Relatórios avançados de todas as falhas e autenticações de validação de usuário.
- Criação de perfis integrada usando identificação DHCP e TCP.
- Suporte virtual e de hardware para aparelhos ESXi e Hyper-V.
- Atualização automática de cluster.
- Mecanismo de entrada avançado de proteção contra ameaças.
- Identificação de atribuição de dispositivos que acessam a rede.

O DIFERENCIAL CLEARPASS

O Gerenciador de Políticas ClearPass é a única plataforma que reforça de forma centralizada todos os aspectos do acesso seguro a nível empresarial para qualquer indústria. O reforço de políticas granulares é baseado na função de um usuário, no tipo e função do dispositivo, no método de autenticação, nos atributos EMM/MDM, no estado do dispositivo, nos padrões de tráfego, na localização e parte do dia.

O ClearPass oferece suporte para infraestrutura de multivendas VPN, com e sem fio, o que permite que a equipe de TI desenvolva políticas de mobilidade seguras em qualquer ambiente de modo fácil.

A escalabilidade de implantação dá suporte para dezenas de milhares de dispositivos e autenticações que ultrapassam as funcionalidades oferecidas por soluções AAA de sistema legado. As opções estão disponíveis tanto para pequenas quanto grandes empresas, em ambientes centralizados e espalhados.

EMISSÃO DE RELATÓRIOS E ALERTAS AVANÇADOS PERCEPTIVOS

O Gerenciador de Políticas inclui funcionalidades de relatórios avançadas por meio de dados personalizáveis, como autenticações, dispositivos com perfis criados, dados de visitante, dispositivos integrados e estados de terminais, tudo em um painel de fácil visualização. Além disso, conta com funcionalidades de alerta granulares.

GERENCIAMENTO DE POLÍTICAS AVANÇADO

Reforço e visibilidade para redes com e sem fio

Com o ClearPass, as empresas podem implementar redes sem fio usando reforço 802.1X com base nos padrões para uma autenticação resistente. O ClearPass também oferece uma maneira de criar políticas não-.1X em redes com fio com o OnConnect, para as empresas que não estejam prontas para utilizar 802.1X e AAA por completo em suas infraestruturas com fios. O ClearPass permite uma abordagem híbrida de modo a permitir que a equipe de TI obtenha as percepções sobre todos os dispositivos, como computadores, smartphones e IoT, que acessam a rede.

Métodos de autenticação concorrentes podem ser utilizados para dar suporte a uma variedade de casos. Também inclui suporte para autenticação de multifatores com base em tempos de login, verificações de comportamento e outros contextos, como usuários ou dispositivos novos, entre outros.

Atribuições para armazenamentos de múltiplas lojas de identidade, como o Active Directory da Microsoft, o diretório compatível com LDAP, a base de dados SQL compatível com ODBC, servidores token e bases de dados internas em diversos domínios podem ser utilizados com uma única política para controle refinado.

Os dados contextuais desses dispositivos com perfis criados permitem que a equipe de TI defina quais dispositivos podem obter acesso à rede VPN, com ou sem fios.

As alterações dos perfis de dispositivos são usadas dinamicamente para modificar privilégios de autorização. Por exemplo, caso um notebook Windows apareça como uma impressora, as políticas ClearPass podem revogar ou negar o acesso automaticamente.

Configuração segura de dispositivos pessoais O ClearPass Onboard fornece provisionamento automático de quaisquer dispositivos Windows, Mac OS X, iOS, Android, Chromebook, e Ubuntu por meio de um portal auto-orientado de usuário. Os SSIDs, certificados de segurança e definições X são configurados automaticamente em dispositivos autorizados.

Gerenciamento personalizável de visitante

O ClearPass Guest simplifica os processos de fluxo de trabalho para que recepcionistas, funcionários e outros membros da equipe que não sejam do TI possam criar contas de usuário temporárias com acesso seguro ao Wi-Fi e à internet com fio. A criação de credenciais de patrocinadores, autorregistro e em massa dão suporte para qualquer necessidade de acesso visitante, como empresarial, varejista, educacional ou um extenso lugar público.

Verificações de integridade do dispositivo

O ClearPass OnGuard utiliza agentes persistentes e dissolvíveis que realizam avaliações avançadas de comportamento de terminais em conexões com ou sem fio e VPN. As funcionalidade de verificação de integridade do OnGuard garantem a conformidade e a proteção da rede antes que os dispositivos sejam conectados.

FUNCIONALIDADE DE GERENCIAMENTO DE POLÍTICAS ADICIONAIS

Integração com sistemas de fluxo de trabalho e segurança A interoperabilidade do ClearPass Exchange inclui APIs com base em REST e encaminhamento de fluxos de dados syslog de e para o ClearPass mediante solicitação que pode ser utilizados para facilitar os fluxos de trabalho com MDM, SIEM, PMS firewalls PMS, call centers, sistemas de admissão e mais. O contexto é compartilhado entre cada componente para reforço e visibilidade da política de ponto a ponto.

Conecte e os apps de trabalho estão prontos para uso

As funcionalidades Auto Sign-On do ClearPass tornam o acesso de apps de trabalho de dispositivos móveis infinitamente mais fácil. Uma autenticação de rede válida conecta os usuários a apps empresariais móveis automaticamente, de modo que estes estejam prontos para funcionar.

O suporte Single sign-on (SSO) opera com Ping, Okta e outras ferramentas de gerenciamento de identidade para melhorar a experiência do usuário em aplicativos com base SAML 2.0.

ESPECIFICAÇÕES

Aparelhos do Gerenciador de Políticas ClearPass

O Gerenciador de Políticas ClearPass está disponível como hardware ou um aparelho virtual que suporta 500, 5.000 e 25.000 dispositivos de autenticação. Os dispositivos virtuais possuem suporte para VMware ESX/i e Microsoft Hyper-V.

- ESX 4.0, ESXi 4.1, até 6.0
- Hyper-V 2012 R2 e Windows 2012 R2 Enterprise

Dispositivos virtuais, bem como os aparelhos de hardware, podem ser implementados com um cluster ativo para aumentar a escalabilidade e a redundância.

Plataforma

- Serviços AAA integrados – RADIUS, TACACS+ e Kerberos
- Autenticação e autorização RADIUS, Web, 802.1X, não-802.1X
- Ferramentas de solução de problemas, analíticas e relatórios avançadas.
- Redirecionamento de portal cativo externo para equipamento de multivendas
- Recursos de modo de monitoramento e simulação de política interativa
- Múltiplos portais de registro de dispositivos – Guest, Aruba AirGroup, BYOD, dispositivos não gerenciados.
- Modelos de implantação para qualquer tipo de rede, loja de identidades e terminais
- Segurança de acesso Admin/Operador via certificados CAC e TLS
- Túneis IPSec

Suporte para protocolos e estrutura

- RADIUS, RADIUS CoA, TACACS+, autenticação 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 e 2, EAP-MD5
- NAC, Microsoft NAP
- Autenticação Windows
- Autenticação MAC
- Auditoria (regras baseadas em varredura de vulnerablidade e portas)
- Online Certificate Status Protocol (OCSP)
- SNMP genérico MIB, SNMP privado MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)
- TLS 1.2

Lojas de identidade suportadas

- Microsoft Active Directory
- RADIUS
- Qualquer diretório compatível com LDAP
- Qualquer servidor SQL compatível com ODBC
- Servidores Token
- Loja de SQL integrada, lista de hospedagem estática
- Kerberos

Padrões RFC

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

Internet drafts

- Versões 0 e 1 Projetadas EAP, Extensões CHAP Microsoft, provisionamento dinâmico utilizando EAP-FAST, TACACS+

Validações de garantia de informação

- FIPS 140-2 – Certificado #2577

Métodos de criação de perfil

- DHCP, TCP, MAC OUI, ClearPass Onboard, SNMP, sensor de dispositivo CIsco

	Aparelho ClearPass 500 (JW770A*)	Aparelho ClearPass 5K (JW771A*)	Aparelho ClearPass 25K (JW772A*)
ESPECIFICAÇÕES DO APARELHO			
Modelo Hardware	Unicom S-1200 R4	Dell R220 XL	Dell R630 XL
CPU	(1) Eight Core 2.4GHz Atom C2758	(1) Quad Core Xeon 3.4GHz E3-1231_V3	(2) Six Core Xeon 2.4GHz E5-2620_V3
Memória	8 GB	8 GB	64 GB
Armazenamento hard drive	(1) SATA (7.3K RPM) 1TB hard drive	(2) SATA (7.2K RPM) 1TB hard drives, controlador RAID-1	(6) SAS (10K RPM) Hard drives Hot-Plug 600GB, controlador RAID-10
Gerenciamento fora de banda	N/A	Controlador Baseboard Management Controller Dell	Dell iDRAC 8 Enterprise
Porta serial	Sim (RJ-45)	Sim (DB-9)	Sim (DB-9)
ESCALABILIDADE DO APARELHO			
Terminais máximos	500	5.000	25.000
FATOR DE FORMA			
Dimensões (LxAxD)	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 máx)	3,85 kg	7,69 kg	Até 16,78 kg
POWER			
Fonte de alimentação	200 watts máx.	250 watts máx.	750 watts máx.
Redundância de alimentação	N/A	N/A	Opcional
Tensão de entrada AC	100/240 VAC auto-selecting	100/240 VAC auto-selecting	100/240 VAC auto-selecting
Frequência de entrada AC	50/60 Hz auto-selecting	50/60 Hz auto-selecting	50/60 Hz auto-selecting
AMBIENTE			
Temperatura de Operação	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)
Vibrações operacionais	0.25 G a 5 Hz até 200 Hz por 15 minutos	0.26 G a 5 Hz até 350 Hz por 15 minutos	0.26 G a 5 Hz até 350 Hz por 15 minutos
Choque operacional	1 pulso de choque de 20 G até 2,5 ms	1 pulso de choque de 31 G até 2,6 ms	1 pulso de choque de 40 G até 2,3 ms
Altitude operacional	-16 m to 3.048 m (-50 pés a 10.000 pés)	-16 m to 3.048 m (-50 pés a 10.000 pés)	-16 m to 3.048 m (-50 pés a 10.000 pés)

* O CP-HW-500 agora é JW770A, o CP-HW-5K agora é JW771A e o CP-HW-25K agora é JW772A.

	Aparelho ClearPass 5K (JX921A)	Aparelho ClearPass 25K (JX920A)
ESPECIFICAÇÕES DO APARELHO		
Modelo Hardware	HPE DL20 Gen 9	HPE DL360 Gen 9
CPU	(1) Xeon 3.5Ghz E3-1240v5 com quatro núcleos (8 Threads)	(2) Xeon 2.4GHz E5-2620_V3 com seis núcleos (12 Threads)
Memória	16 GB	64 GB
Armazenamento hard drive	(2) SATA (7.2K RPM) 1TB hard drives, controlador RAID-1	(6) SAS (10K RPM) 600GB Hot-Plug hard drives, controlador RAID-10
Gerenciamento fora de banda	HPE Integrated Lights-Out (iLO) Padrão	HPE Integrated Lights-Out (iLO) Avançado
Porta serial	Sim (Virtual Serial via iLO)	Sim (DB-9)
ESCALABILIDADE DO APARELHO		
Pontos finais máximos	5,000	25,000
FATOR DE FORMA		
Dimensões (LxAxD)	17.11" x 1.70" x 15.05"	17.1" x 1.7" x 27.5"
Peso (Config máx)	Até 19.18 Lbs	Até 33.3 Lbs
POWER		
Fonte de alimentação	HPE 900W AC 240VDC Módulo FIO de Entrada de Alimentação*	HPE 500W Flex Slot Platinum Fonte de Alimentação Hot
Redundância de alimentação	Opcional	Opcional
Tensão de entrada AC	100/240 VAC auto-selecting	100/240 VAC auto-selecting
Frequência de entrada AC	50/60 Hz auto-selecting	50/60 Hz auto-selecting
AMBIENTE		
Temperatura de Operação	10° a 35°C (50° a 95°F)	10° C a 35° C (50° F a 95° F)
Vibrações operacionais	Vibração aleatória a 0.000075 G²/Hz, 10Hz to 300Hz, (0.15 G's nominal)	Vibração aleatória a 0.000075 G²/Hz, 10Hz to 300Hz, (0.15 G's nominal)
Choque operacional	2 G's	2 G's
Altitude operacional	3,050 m (10,000 ft).	3,050 m (10,000 ft)

* A Fonte de Alimentação Redundante HPE 900W possui suporte para 100VAC a 240VAC e também para 240VDC.

ORIENTAÇÃO PARA PEDIDOS

Solicitar um Gerenciador de Políticas ClearPass envolve dois passos:

1. Determinar o número de dispositivos/terminais autenticados em seu ambiente. E, além disso, escolher a funcionalidade opcional, como visitantes por dia, total de dispositivos BYOD sendo configurados para uso empresarial e número total de computadores que precisam de verificações de integridade.
2. Escolha a plataforma apropriada (seja uma ferramenta virtual ou hardware) para acomodar o total de dispositivos e usuários que precisarão de autenticação.

OBSERVAÇÃO: Os equipamentos virtuais devem ser fornecidos com os mesmos recursos para corresponder às especificações de aparelhos de hardware.

INFORMAÇÕES DE PEDIDO

Código do Produto	Descrição
Aparelhos de hardware	
JW770A	Aparelho V2 HW Aruba ClearPass 500 Terminais Únicos com 25 Licenças Empresariais
JW771A	Aparelho HW V3 Aruba ClearPass 5000 Terminais Únicos com 25 Licenças Empresariais
JW772A	Aparelho HW V3 Aruba ClearPass 25000 Terminais Únicos e Inc 25 Licenças Empresariais
JX921A	Aparelho de Hardware Aruba ClearPass DL20 5000 Terminais Únicos e 25 Licenças Empresariais
JX920A	Aparelho de Hardware Aruba ClearPass DL360 25000 Terminais Únicos e 25 Licenças Empresariais
Aparelhos Virtuais	
JW335AAE	Aparelho Virtual E-LTU Aruba ClearPass 500 Terminais Únicos com 25 Licenças Empresariais
JW336AAE	Aparelho Virtual E-LTU Aruba ClearPass 5000 Terminais Únicos com 25 Licenças Empresariais
JW337AAE	Aparelho Virtual E-LTU Aruba ClearPass 25000 Terminais Únicos com 25 Licenças Empresariais
Fontes de Alimentação	
JW790A	Fonte de Alimentação Spr 750W Aruba AWCP-HW630-PSU
JX923A	Fonte de Alimentação Reserva DL20 Aruba ClearPass DL20
JX922A	Fonte de Alimentação Reserva 500W DL360 Aruba ClearPass-Airwave
Software de aplicativo expansível*	
ClearPass Onboard – gerenciamento de certificado e configuração do dispositivo	
ClearPass OnGuard – integridade de terminais do dispositivo	
ClearPass Guest – gerenciamento de acesso de visitantes	
Garantia	
Hardware	1 ano peças/assistência**
Software	90 dias**

* O software de aplicativo expansível está disponível com os seguintes incrementos: 100, 500, 1.000, 2.500, 5.000, 10.000, 25.000, 50.000 e 100.000.

** Prorrogável meidante contratação de suporte

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/latam