DIRECCIÓN DE TECNOLOGIA DE LA INFORMACIÓN Y COMUNICACION

Santo Domingo, R.D
26 de Julio 2024

Al : **Licda. Betty Gerónimo**
Alcaldesa (ASDN)

Vía : **Licdo. Wendy Oscar Fortunato**
Director Administrativo

Atención : **Licdo. Pedro Montero**
Encargado de compra

Asunto : **Solicitud de comprar.**

AYUNTAMIENTO SANTO DOMINGO NORTE
DIRECCION ADMINISTRATIVA
República Dominicana
GESTION 2024-2028

Después de un cordial saludo, me dirijo a ustedes con la finalidad de solicitar la compra de un **Ubiquiti Dream Machine Pro, para la seguridad y monitoreo de red.**

Se anexa informe de incidentes de seguridad de red, descripción y cotización del dispositivo solicitado.

Sin otro particular se despide.

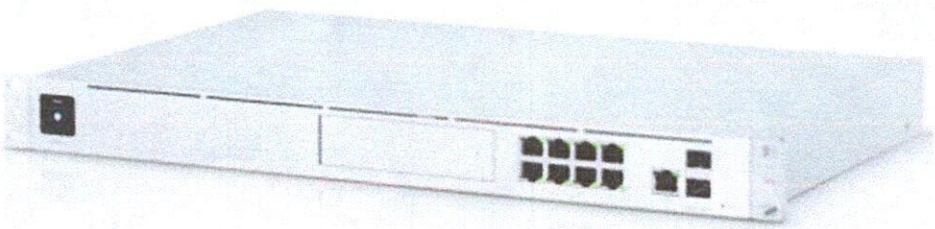
AYUNTAMIENTO
Departamento de Tecnología de la Información y Comunicaciones
República Dominicana
SANTO DOMINGO NORTE

Licdo. Misael Henríquez
Director de tecnología

DEPARTAMENTO DE COMPRAS
RECIBIDO
Firma
Fecha: 29-7-24 Hora: 10:15 am

Descripción de dispositivo solicitado

Ubiquiti Dream Machine Pro



Mechanical

Dimensions 442.4 x 43.7 x 285.6 mm (17.4 x 1.7 x 11.2")

Weight 3.9 kg (8.6 lb)

Enclosure material Aluminium CNC, SGCC steel

Mount material SGCC steel

Hardware

Processor Quad-core ARM® Cortex®-A57 at 1.7 GHz

System memory 4 GB DDR4

On-board storage 16 GB eMMC

Management interface Ethernet

Bluetooth

Networking interface LAN:

(8) GbE RJ45 ports

(1) 10G SFP+ port

WAN:

(1) GbE RJ45 port

(1) 10G SFP+ port

IDS/IPS throughput 3.5 Gbps*

*Measured with iPerf3 on a DHCP network. Performance may be reduced with PPPoE depending on ISP implementation.

Power method (1) Universal AC input, 100—240V AC, 50/60 Hz

(1) USP-RPS DC input

Power supply AC/DC, internal, 50W

Supported voltage range 100—240V AC

Max. power consumption 33W

ESD/EMP protection Air: ± 15kV, contact: ± 8kV

LCM display (1) 1.3" touchscreen

Button Factory reset

Ambient operating temperature -10° to 40° C (14° to 104° F)

Ambient operating humidity 5 to 95% noncondensing

Certifications CE, FCC, IC

Gateway Features

Performance	Redundant WAN with failover and load balancing
	WiFi QoS with UniFi APs
	Application, domain, and country-based QoS
	Application and device type identification
	Additional internet failover with LTE Backup
	Internet quality and outage reporting
Next-generation security	Application-aware firewall rules
	Signature-based IPS/IDS threat detection
	Content, country, domain, and ad filtering
	VLAN/subnet-based traffic segmentation
	Full stateful firewall
Advanced networking	License-free SD-WAN
	WireGuard, L2TP and OpenVPN server
	OpenVPN client
	OpenVPN and IPsec site-to-site VPN
	One-click Teleport and Identity VPN
	Policy-based WAN and VPN routing
	DHCP relay
	Customizable DHCP server
	IGMP proxy
	IPv6 ISP support

AYUNTAMIENTO SANTO DOMINGO NORTE
RNC 425000339

JUNTOS POR UN NUEVO norte
Gestión 2024-2028

Informe de Incidente de Seguridad en la Red

Resumen

Durante el día de ayer, se registraron intentos de asimilar los Access Points (AP) de la institución en dos ocasiones. El primer intento tuvo lugar a las 10 de la mañana, seguido de dos intentos a las 4 de la tarde. Debido a la ausencia de un Dispositivo de Monitoreo de Red (UDM), la identificación del actor responsable se ha vuelto un desafío. No obstante, se presume que dichos intentos fueron realizados internamente, ya que en una ocasión paso lo mismo y el sistema bloqueo al usuario

Detalles del Incidente

El primer intento de asimilación de los Access Points (AP) se produjo a las 10 de la mañana, el cual nos llevó que al medio día tuvimos que reiniciar todo el sistema para restaurarlo, seguido de dos intentos adicionales a las 4 de la tarde. La falta de un Dispositivo de Monitoreo de Red (UDM) ha complicado la identificación del autor de dichas acciones. Dadas las circunstancias, se infiere que los intentos fueron realizados desde el interior de la red, lo que plantea preocupaciones sobre la integridad del personal.

Recomendaciones

Ante la incertidumbre acerca del origen de los intentos de asimilación de los Access Points, se hace imperativo implementar medidas de seguridad adicionales. Se sugiere la adquisición e instalación de un Dispositivo de Monitoreo de Red (UDM) para una supervisión constante de la red. Asimismo, se recomienda realizar una exhaustiva revisión de las políticas de seguridad informática y llevar a cabo una formación específica para el personal involucrado en la gestión de la red.

Conclusión

La seguridad de la red de la institución se ve comprometida ante los recientes intentos de asimilación de los Access Points. Es fundamental abordar este incidente con prontitud y adoptar medidas proactivas para prevenir posibles vulnerabilidades y proteger la integridad de los sistemas informáticos. Se insta a toda la comunidad institucional a colaborar en el fortalecimiento de la seguridad cibernética y a mantener una constante vigilancia frente a posibles amenazas internas y externas.

Luis A. Ovalle

Administrador de Seguridad Electrónica

Origina Director de tecnología

Copia Asesora de tecnología

AYUNTAMIENTO SANTO DOMINGO NORTE
Departamento de Tecnología de la Información y Comunicación
República Dominicana