



Vista previa de la presentación

Avril Alonso – Team Captain HTTS Security
Julio Román – Escalation Engineer HTTS Security

<https://bit.ly/CL3es-jun24>



Webinar Community Live - Comunidad de Cisco

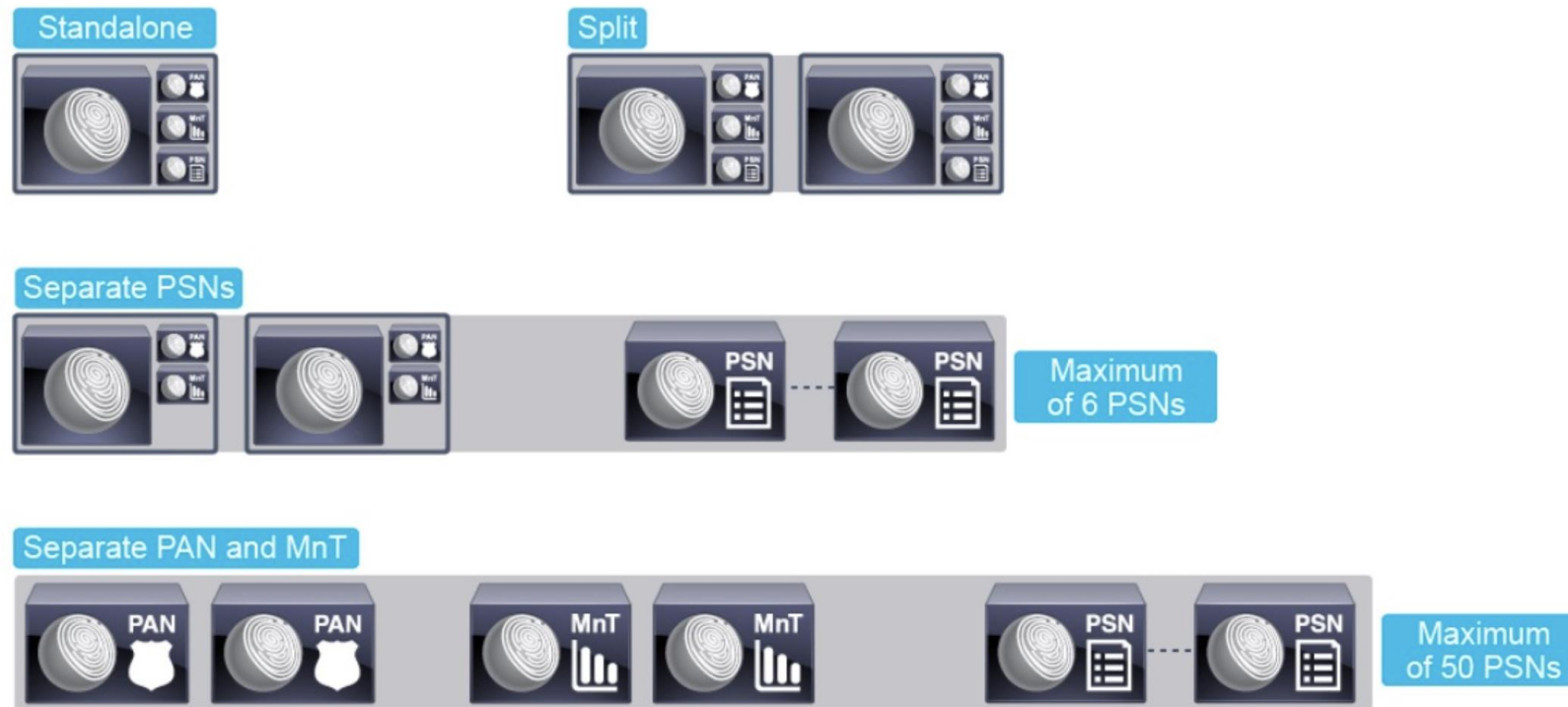
Implementación y Configuración de Cisco ISE

Exploraremos las consideraciones clave para realizar actualizaciones exitosas en Cisco Identity Services Engine (ISE) y los Firewall (NGFW) de Cisco. Mejores prácticas, los desafíos comunes y las estrategias recomendadas. ¡No se lo pierda!

Jueves 20 de Junio 2024

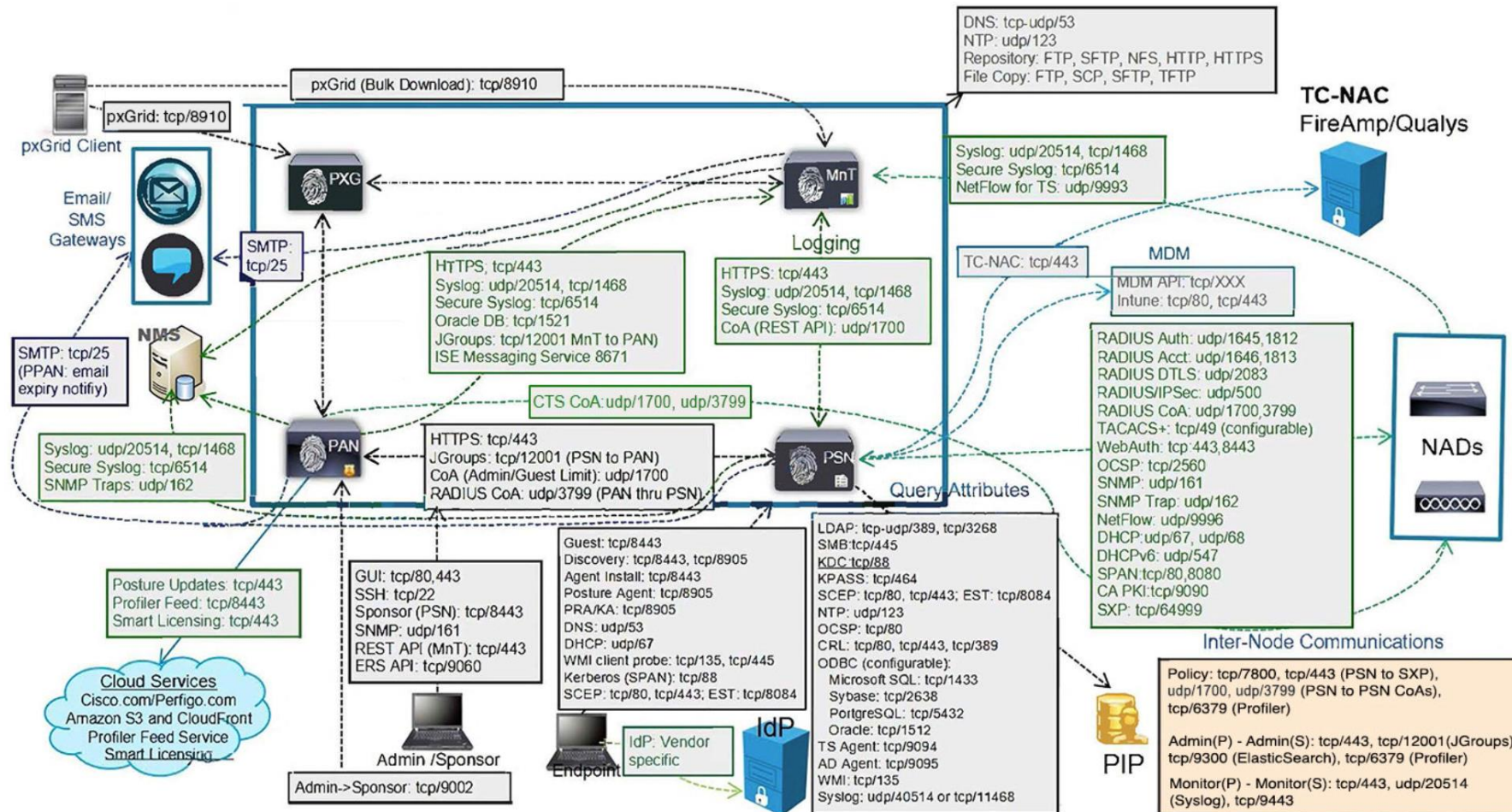
Opciones de implementación ISE

El modo predeterminado para ISE cuando se implementa por primera vez es el modo independiente (Standalone). Este modo tiene todas las personas activas en un solo nodo y no proporciona redundancia en caso de falla.



ISE Modelo de comunicación y puertos

Esta figura ilustra las comunicaciones entre varios componentes y puertos de Cisco ISE.



Tipo de Autenticación

- **Supplicant**, es un cliente capaz para 802.1x también conocido como Dot1x, por ejemplo, Cisco AnyConnect NAM, o el Supplicant nativo de MS Windows.
- Un **Authenticator** es un dispositivo de acceso a la red (NAD), como switches o WLCs los cuales procesan paquetes EAP desde el cliente / endpoint, facilitando la comunicación entre este y los servidores de AAA.
- **MAB** (MAC Address Bypass), es un método para autenticar y autorizar clients / endpoints que no son capaces de autenticar un método y autorizar endpoints que no son compatibles o no están habilitados para 802.1x.

	802.1X	MAB	WebAuth
802.1X capable Employee	√	X	√
Non-802.1X Managed device	X	√	X
802.1X or non-802.1X Contractor	X	X	√
802.1X or non-802.1X IP phones	√	√	X

ISE Live log

Cuando ISE busca hacer coincidir una solicitud de acceso con el conjunto de políticas correcto, recuerde que las condiciones utilizadas para hacer coincidir el conjunto de políticas se leen en orden de arriba hacia abajo.

The screenshot displays the ISE Live log interface with several callouts and detailed views:

- Callout 1:** Points to the 'Authenticat' column header, labeled 'Match Incorrect Policy Set'.
- Callout 2:** Points to the 'Details' button, labeled 'Details'.
- Callout 3:** Points to the 'Device Type' field in the details view, labeled 'Device Type for NAD is "Wired"'. The value is 'All Device Types#Wired'.
- Callout 4:** Points to the 'Conditions' column in the policy set table, labeled 'Conflicting Conditions in Policy Sets'. It highlights two conditions: 'DEVICE Device Type EQUALS All Device Types#Wireless'.

Status	Endpoint ID	Authenticat	Authenticat	Authorizati	IP Address	
❌	employee1	00:50:56:8E:56:02	HQ Policy ...	HQ Policy ...	DenyAccess	10.10.30.11
✅	employee1	00:50:56:8E:56:02	Wired Acc...	Wired Acc...	Employee ...	10.10.30.11

Status	Policy Set Name	Description	Conditions
✅	HQ Policy Set		DEVICE Device Type EQUALS All Device Types#Wireless
✅	Wired Access Policy		DEVICE Device Type EQUALS All Device Types#Wireless
✅	Wireless Access Policy		DEVICE Device Type EQUALS All Device Types#Wireless

Field	Value
Audit Session Id	0A0A0A0300000
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPV2)
Service Type	Framed
Network Device	3k-access
Device Type	All Device Types#Wired
Location	All Locations#HQ
NAS IPv4 Address	10.10.10.3
NAS Port Id	GigabitEthernet1/0/3
NAS Port Type	Ethernet
Authorization Profile	DenyAccess
Response Time	52 milliseconds

Buscamos nuevos expertos para traer más temas...
¡No se pierda nuestro próximo webinar el jueves 20 de junio!

 [¡Inscríbese ahora!](#)

Nuestros eventos anteriores



[Un vistazo a Cisco XDR, Seguridad Centralizada contra Amenazas y Vulnerabilidades](#)

Seguridad / 6 Junio 2024

Brenda Márquez, Jorge Navarrete y Uriel Zamora

Una vista práctica a la solución de Cisco Extended Detection and Response (XDR), donde se abordaron temas como tipos de licencia, integraciones, y casos de uso más comunes. Compartimos algunos "TAC Tips" del TAC global de Cisco sobre automatización, visibilidad, resolución de problemas frecuentes y más. Compartimos los secretos detrás de una implementación exitosa para fortalecer su infraestructura de seguridad con consejos directos de los expertos en la materia.



[Migración de Fabric Interconnects 6200 a Modelos 6400/6500](#)

Data Center / 30 Mayo 2024

Jaime Islas y Leonardo J. Rosales

Abordaremos el proceso de migración de los Fabric Interconnects de segunda generación hacia los modelos más recientes de cuarta y quinta generación. Juntos, revisamos todas las consideraciones, tanto físicas como de configuración, a tomar en cuenta antes, durante y después del proceso de migración.