Prácticas recomendadas para la implementación de Zero Trust con Palo Alto Networks

9.1

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 18, 2019

Table of Contents

Prácticas recomendadas para Zero Trust

Este documento describe qué es una estrategia Zero Trust y cómo implementarla en su red utilizando una metodología de cinco pasos que le guía a través de las prácticas recomendadas para identificar sus superficies de protección críticas, definir sus flujos de transacciones críticas, diseñar su red Zero Trust, crear su política de Zero trust y mantener dicha implementación. Las secciones incluyen enlaces a información detallada de Palo Alto Networks, incluido cómo configurar cortafuegos de última generación (físicos y virtuales) y capacidades de seguridad de Palo Alto Networks para evitar la vulneración de datos.

© 2019 Palo Alto Networks, Inc.

¿Qué es Zero Trust y por qué lo necesito?

Zero Trust es un enfoque estratégico y orientado a los negocios para asegurar sus datos, aplicaciones, activos y servicios (DAAS) más críticos, así como a sus usuarios, en función de lo que es importante para su negocio en particular, en una *superficie de protección*. La estrategia Zero Trust es neutral en cuanto a infraestructura, por lo que puede aplicarla en todas las ubicaciones físicas y virtuales: red, nube pública, nube privada y endpoint. El concepto detrás de Zero Trust es simple: la confianza (Trust) es una vulnerabilidad. No confíe en nada en el entorno digital (paquetes, identidades, dispositivos o servicios) y compruébelo todo. No existe la confianza predeterminada.

La implementación de la estrategia no es algo que se hace una vez y que copia de una red a otra, porque cada entorno y superficie de protección es diferente; y a medida que las empresas cambian con el tiempo, el objetivo y los elementos DAAS también cambian. La estrategia es específica de los negocios y la estrategia de seguridad es específica para proteger lo que es importante para su negocio en particular.

El objetivo de la estrategia Zero Trust es eliminar la confianza de la red. La eliminación de la confianza ayuda a evitar infracciones de datos exitosas, simplifica las operaciones a través de la automatización y una base de reglas reducida, y simplifica el cumplimiento normativo y las auditorías porque los entornos Zero Trust están diseñados para facilitar el cumplimiento y las auditorías.

© 2019 Palo Alto Networks, Inc.

Punto de vista de Zero Trust

Cuando entienda Zero Trust, verá la confianza por lo que es, una vulnerabilidad que los atacantes aprovechan. Los atacantes pueden robar credenciales, falsificar información en encabezados de paquetes e incluso ser empleados o socios "de confianza". Edward Snowden era un usuario fiable que tenía el software de antivirus adecuado y el nivel de revisión correcto en su estación de trabajo. También utilizó la autenticación de múltiples factores. Pero a nadie le importó a dónde iba en la red o los paquetes que generaba porque era un usuario de confianza, por lo que él podía explorar la red, encontrar y filtrar datos confidenciales. La lección es que el resultado de la confianza digital es la traición digital; no confíe en identidades, aplicaciones o datos. Cuando adopta el punto de vista Zero Trust, usted:

- Alinea la seguridad con las funciones empresariales porque las funciones empresariales determinan lo que necesita proteger.
- Inspeccione y registre todos los paquetes en la Capa 7 cuando accedan a un recurso.
- Acceda a todos los recursos de manera segura, independientemente de su ubicación.
- Aplique una política de seguridad coherente en todas las ubicaciones.
- Gestione la política de seguridad y segmentación de forma centralizada.
- Adapte los cambios a medida que cambia su negocio.

La confianza es un punto de fracaso que puede evitar si implementa una estrategia Zero Trust.

- Prácticas recomendadas de alto nivel de Zero Trust
- ¿Cómo inicio mi implementación de Zero Trust?

Prácticas recomendadas de alto nivel de Zero Trust

Las siguientes prácticas recomendadas le preparan y le ayudan a llevar a cabo la transición de su red a una arquitectura Zero Trust:

- Defina los resultados comerciales deseados antes de diseñar su entorno Zero Trust. El modelo Zero Trust admite y habilita funciones comerciales seguras.
- Diseñe desde adentro hacia afuera en lugar de lo contrario para proteger primero lo que es más valioso para su negocio. Es más probable que sus activos más valiosos estén en su centro de datos que en su perímetro.
- Utilice una plataforma integrada y gestionada de forma central que reduzca el coste total de propiedad, en lugar de una colección de productos específicos que no funcionan bien juntos. Palo Alto Networks comparte información entre los elementos de la plataforma y permite una gestión centralizada y una operación simplificada utilizando Panorama, GlobalProtect y Prisma Access para proporcionar políticas, prevención y protección coherentes en todas las ubicaciones.
- Utilice los cortafuegos de última generación de Palo Alto Networks como gateways de segmentación para consolidar las tecnologías de seguridad en una plataforma y aplicar una política de seguridad coherente en todas las ubicaciones de forma nativa en la capa 7 utilizando App-ID, User-ID y Content-ID. Un gateway de segmentación segmenta y controla la red en función de las aplicaciones, los usuarios y los datos, y debe proporcionar un control de acceso granular y asegura todo el tráfico a medida que cruza los microperímetros y obtiene acceso a una superficie de protección.

  No necesita cambiar su infraestructura para crear microperímetros porque crea estos microperímetros en la misma política de la Capa 7 al permitir que solo los usuarios autorizados accedan solo a las superficies de protección que necesitan para fines comerciales.
- Segmente su red en función de lo que es valioso para su negocio, para evitar movimientos laterales no autorizados.

© 2019 Palo Alto Networks, Inc.

- Aplique el principio de mínimo privilegio de acceso a sus superficies de protección. Determine quién necesita acceso a qué recursos, cómo necesitan el acceso y cuándo necesitan acceder. Permita solo el nivel exacto de acceso requerido para cada usuario y dispositivo, reivindique la identidad (incluidas las autorizaciones adecuadas) y luego asigne la política de Capa 7 a la identidad.
- Descifre, inspeccione y registre cada paquete a través de la Capa 7 en conformidad con lo que las regulaciones, el cumplimiento normativo y sus prácticas comerciales le permiten inspeccionar. Debe inspeccionar y registrar el tráfico de Capa 7. Recuerde, cada atacante sabe cómo evitar los controles de seguridad en la Capa 3 y la Capa 4.
- Cree una estrategia para etiquetar cargas de trabajo para agrupar objetos y registrar etiquetas dinámicamente para ayudar a automatizar la política de seguridad.
- Desarrolle procesos para operar, mantener y actualizar continuamente los controles de prevención a medida que desarrolla su estrategia y diseña la red. Documente los procesos, eduque y de formación al personal, establezca puntos de referencia y mida el progreso con respecto a dichos puntos.
- Lleve a cabo una transición hacia un entorno de Zero Trust gradualmente, empezando con uno o más segmentos no críticos de los cuales puede aprender y ganar experiencia. Los segmentos de Zero Trust coexisten con segmentos anteriores, por lo que puede utilizar un enfoque seguro e iterativo en lugar de un enfoque arriesgado de extracción y sustitución.

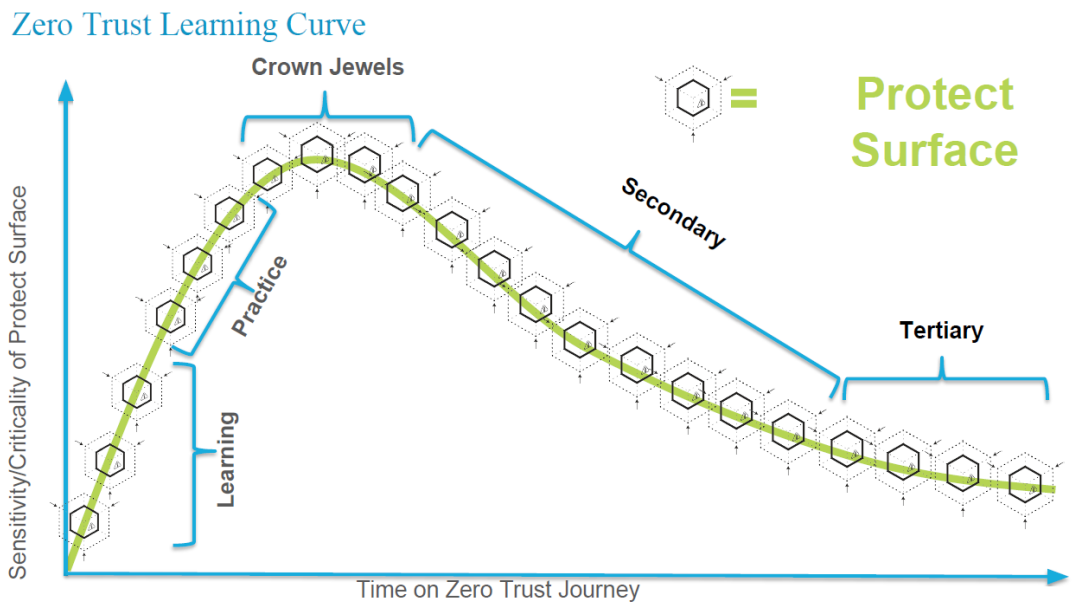
A medida que disminuye la importancia de las aplicaciones, puede ser menos agresivo con la protección. Por ejemplo, no necesita aplicar la misma protección a una aplicación de chat que debe aplicar a aplicaciones críticas para el negocio. La colaboración con líderes empresariales ayuda a determinar qué aplicaciones son las más críticas para proteger.

¿Cómo inicio mi implementación de Zero Trust?

La educación y la colaboración inician el viaje hacia la seguridad de Zero Trust. Usted y otras partes interesadas que identificarán lo que es valioso para su negocio y cómo protegerlo deben comprender los conceptos, principios y objetivos de Zero Trust.

1. Crear un centro Zero trust para la excelencia. Este es un equipo multifuncional de líderes empresariales (tomadores de decisiones empresariales y técnicas), TI, seguridad de la información, infraestructura, desarrolladores de aplicaciones y otros interesados. El equipo define e identifica cada superficie de protección y los datos, aplicaciones, activos y servicios (elementos DAAS) que conforman cada superficie de protección. Priorizan las superficies de protección más valiosas para su negocio y planifican e implementan la estrategia Zero Trust. El equipo mantiene su colaboración mediante el mantenimiento de la implementación a medida que cambia el negocio. Los líderes empresariales pueden hablar sobre los resultados comerciales deseados, los requisitos de cumplimiento y el valor de los activos comerciales.
2. Asista a un taller de Zero Trust para preparar a todos para que mantengan una misma línea. Póngase en contacto con su representante de ventas de Palo Alto Networks para obtener más información y programar un taller.
3. Siga La metodología de cinco pasos para definir la red segmentada que desea construir.
4. Comience la transición con uno o más segmentos pequeños, bien entendidos, de bajo riesgo (no críticos para las operaciones comerciales) para aprender de la experiencia. No comience con activos críticos. Luego, pruebe su aprendizaje en uno o más segmentos de práctica. Cuando se sienta listo, coloque sus superficies de protección más críticas para el negocio (los elementos DAAS que conforman la superficie de protección) en microperímetros Zero Trust, un microperímetro por superficie de protección. Después de eso, convierta el siguiente conjunto más valioso de superficies de protección a Zero Trust, etc.

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

La metodología de cinco pasos

La metodología de cinco pasos para implementar una estrategia Zero Trust presenta un camino claro y lógico para proteger su entorno, sus datos, las aplicaciones, los activos, los servicios y los usuarios. La forma en la que aplica la metodología depende de lo que está protegiendo y de los requisitos de su negocio —lo que es crítico para su negocio— pero los resultados que se desean obtener son los mismos:

- Segmente la red de manera efectiva y eficiente para evitar el movimiento lateral.
- Proteja los datos y sistemas críticos para el negocio frente a aplicaciones y usuarios no autorizados.
- Proteja las aplicaciones críticas para el negocio frente al acceso y uso no autorizados.
- Aplique la política en la red, la nube y los endpoints sin interrupciones, para simplificar la gestión y aplicar una política coherente en todas partes.

La metodología de cinco pasos funciona tanto si implementa una estrategia Zero Trust en la nube, en una red privada o en los endpoints, independientemente de la infraestructura.

PASO 1: Defina su superficie de protección

Una superficie de protección es lo más valioso para su negocio: los datos, las aplicaciones, los activos y los servicios (DAAS) que necesita proteger para garantizar el funcionamiento normal del negocio. La definición de su superficie de protección le permite concentrarse en defender lo que realmente le importa a su negocio en lugar de tratar de identificar y proteger toda la superficie de ataque o centrarse solo en el perímetro. La superficie de protección también es mucho más pequeña que la superficie de ataque o el perímetro, por lo que es más fácil de proteger.

Defina su superficie de protección en función de los elementos DAAS más cruciales para su negocio:

- **D**atos. ¿Qué datos deben protegerse? Piense en la propiedad intelectual, como el código o los procesos patentados; la información de identificación personal (PII); la información de la tarjeta de pago (PCI) y la información sanitaria personal (PHI), como la información de la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA).
- **A**plicaciones. ¿Qué aplicaciones hacen uso de información confidencial? ¿Qué aplicaciones son críticas para las funciones de su negocio?
- **A**ctivos. ¿Qué activos son los más importantes? Dependiendo de su negocio, podrían ser controles SCADA, terminales de POV, equipos médicos, equipos de fabricación y grupos de servidores críticos.
- **S**ervicios. ¿Qué servicios pueden explotar los atacantes para interrumpir las operaciones de TI y afectar negativamente al negocio, como DNS, DHCP y Active Directory?

Cada elemento DAAS crítico es parte de una superficie de protección (o en algunos casos es una superficie de protección). Por ejemplo, si su empresa proporciona atención médica, entonces la información médica protegida (PHI) es crítica para su empresa. Los *Datos* son la información del paciente. Las *Aplicaciones* son las aplicaciones que se utilizan para acceder a la información de PHI, por ejemplo, EPIC. Los *Activos* son servidores que almacenan los datos y el equipo que genera la PHI, como escáneres médicos o estaciones de trabajo de médicos. Los *Servicios* son servicios que se utilizan para acceder a los datos, como el inicio de sesión único y Active Directory.

A medida que siga la metodología de cinco pasos, colocará cada superficie de protección en su propio microperímetro (segmentado por un cortafuegos físico o virtual de última generación de Palo Alto Networks, que actúa como una puerta de enlace de segmentación) para que controle exactamente quién

© 2019 Palo Alto Networks, Inc.

accede al elemento, cómo acceden a él y cuándo acceden a él. Asegure cada superficie de protección de la manera más adecuada para dicha superficie de protección. Un microperímetro es más fácil de gestionar y defender que un amplio perímetro que abarca elementos DAAS que los usuarios con diferentes requisitos de acceso necesitan alcanzar. También traslada las protecciones más cerca de los datos críticos.

Priorice qué proteger primero en función de lo que es crítico para gestionar su negocio. Sus activos más valiosos suelen estar en su centro de datos o en la nube. Después de implementar Zero Trust en una o más superficies de protección no críticas para obtener experiencia, proteja sus superficies de protección más críticas. Es posible que no conozca todas las aplicaciones en su centro de datos cuando comience, pero seguro que sí conoce sus aplicaciones más críticas. Más adelante, pase al siguiente conjunto de superficies de protección en la lista de prioridades y siga revisando la lista hasta alcanzar sus objetivos de seguridad.

Use las siguientes herramientas para obtener visibilidad del tráfico de su red y ayudar a identificar los elementos DAAS que conforman sus superficies de protección más críticas:

- El conocimiento del equipo acerca del negocio. Por ejemplo, los líderes empresariales pueden hablar sobre el valor estratégico de las aplicaciones.
- Implemente uno o más cortafuegos de última generación de forma transparente en su red en el modo cable virtual (vwire), un modo de transferencia que no requiere cambios de topología porque las interfaces vwire no tienen direcciones IP o MAC, para obtener visibilidad en el tráfico. Compruebe los Logs de tráfico para ver y analizar el tráfico de red. Si ya cuenta con cortafuegos gestionados en su red, use los logs de Panorama.
- Vea los logs en Cortex Data Lake y use herramientas de descubrimiento de activos de terceros que funcionen con Cortex de uno de los socios integrados de Palo Alto Networks.
- Utilice Prisma SaaS para descubrir usuarios, activos y datos para aplicaciones SaaS y obtener visibilidad sobre esas aplicaciones.
- Si ejecuta PAN-OS 9.0 o posterior en el cortafuegos de última generación o en el Panorama que gestiona sus cortafuegos, utilice el optimizador de políticas Policy Optimizer para ayudar a identificar aplicaciones clave en las reglas de política de seguridad existentes. (Policy Optimizer incluso le muestra todas las aplicaciones en reglas basadas en puertos). Si no puede usar Policy Optimizer, utilice Expedition para obtener visibilidad sobre las aplicaciones.
- Herramientas de asignación de dependencia de aplicaciones para descubrir las dependencias de las aplicaciones (los recursos que una aplicación usa, como bases de datos, balanceadores de carga, servidores, etc.) automáticamente.

Paso 2: Defina los flujos de transacciones en su superficie de protección

Defina los flujos de transacción (interacciones) entre sus elementos DAAS críticos y los usuarios para comprender sus interdependencias: quién tiene razones comerciales para acceder a cada elemento, de qué manera y en qué momento. Defina los flujos de transacciones para comprender y diseñar la red. La definición de mapas le ayuda a comprender cómo crear una política de seguridad que permita que solo los usuarios autorizados accedan a datos y activos específicos utilizando las aplicaciones especificadas (principio de mínimo privilegio de acceso).

Hay muchas formas de asignar flujos de transacciones, y algunas técnicas para definir su superficie de protección también se aplican a la asignación de sus flujos de transacciones:

- Aproveche los diagramas de flujo existentes si los tiene (el cumplimiento normativo y las auditorías a veces requieren que las empresas creen diagramas de flujo).
- Trabaje con expertos en arquitecturas de aplicaciones, redes y empresas, y representantes empresariales para comprender el propósito de las aplicaciones y el flujo de transacciones que imaginan los arquitectos y representantes de empresa.
- Introduzca uno o más cortafuegos de última generación de forma transparente en su red en modo cable virtual (vwire) para obtener visibilidad sobre el tráfico. Revise Logs de tráfico para ver y analizar el tráfico.

© 2019 Palo Alto Networks, Inc.

- Utilice herramientas de terceros de socios integrados de Palo Alto Networks.
- Utilice la información de logs provenientes de Cortex Data Lake para obtener visibilidad y asignar flujos de transacciones. Cortex Data Lake agrega logs del cortafuegos de última generación, cortafuegos VM-Series, Prisma Access y Traps.
- Para las aplicaciones, asigne los flujos de trabajo, incluido el flujo de datos de la aplicación a través de la red, los objetos informáticos necesarios para cada aplicación y quién utiliza cada aplicación.
- Para los datos, averigüe quién usa los datos, dónde los recopila, almacena, usa y transfiere, y cómo se almacenan, cifran, archivan o destruyen los datos después de su uso.
- Para los activos, averigüe la ubicación del activo, quién lo usa, cuándo lo usa y dónde encaja el activo en los flujos de trabajo.
- Para los servicios, asigne los flujos de trabajo del servicio en todo el entorno.

Además de revelar quién usa qué aplicaciones dónde y cuándo, la definición de los flujos de transacciones proporciona una visibilidad granular que ayuda con la planificación y el cumplimiento de la recuperación ante desastres. También le brinda la oportunidad de optimizar los flujos de trabajo y examinar quién tiene razones comerciales legítimas para acceder a los elementos DAAS en cada superficie de protección.

Cuando comprenda los flujos de transacciones a través de su red, sabrá cómo segmentar la red y dónde insertar los controles porque comprenderá quién usa cada superficie de protección, cómo la usa, dónde está ubicada y qué elementos interactúan para habilitar cada aplicación crítica.

Paso 3: Diseñe una red de Zero Trust

Armado con un conocimiento de su superficie de protección y flujos de transacciones, comience a diseñar su red Zero Trust en función de lo que es valioso para su negocio. Diseñe las superficies de protección críticas para el negocio que ha identificado en PASO 1: Defina su superficie de protección desde adentro hacia afuera. A medida que desarrolla la arquitectura, tenga en cuenta la facilidad de operación y mantenimiento, y la flexibilidad para acomodar los cambios en la superficie de protección y en los negocios. Ejecute la Herramienta de evaluación prácticas recomendadas para establecer una línea base de configuración de prácticas recomendadas y medir el progreso hacia sus objetivos de Zero Trust.

La piedra angular de la arquitectura son las puertas de enlace de segmentación; cortafuegos de última generación físicos o virtuales de Palo Alto Networks que conectan sus segmentos de red y hacen cumplir la política de Capa 7. Ejecute todo el tráfico a través de una puerta de enlace de segmentación, coloque las puertas de enlace de segmentación lo más cerca posible de los recursos que protegen y utilícelas junto con otras capacidades de Palo Alto Networks para automatizar tanto como sea posible. Cortafuegos de última generación:

- Cree un microperímetro en política de Capa 7 alrededor de cada superficie de protección. Esto evita el movimiento lateral porque el microperímetro proporciona controles de políticas granulares para quién (User-ID) accede a qué aplicaciones (App-ID) y recursos de qué manera (Content-ID) y en qué momento a través de la puerta de enlace de segmentación. Segmente en función de cómo fluyen las transacciones en su red y cómo sus usuarios y aplicaciones acceden a datos y servicios.
- Añada capacidades de seguridad en un único punto de control para todo el tráfico que entra y sale de la superficie de protección. La puerta de enlace de segmentación deberá aplicar políticas, descifrar el tráfico cifrado y aplicar protecciones como:
    - Seguridad de DNS (use el servicio de seguridad de DNS, que proporciona múltiples fuentes de información de amenazas en tiempo real, análisis en tiempo real infinitamente ampliable de solicitudes de DNS y firmas de DNS avanzadas).
    - Prevención de intrusiones (Protección frente a vulnerabilidades, antispyware y perfiles de antivirus).
    - Bloqueo de tipos de archivos potencialmente peligrosos.
    - Prevención de amenazas desconocidas y del día 1 (WildFire).
    - Filtrado de URL.
    - Prevención de pérdida de datos (DLP).
- Descifrado e inspección de tráfico en la Capa 7 en tiempo real.

© 2019 Palo Alto Networks, Inc.

- Registre cada paquete desde la capa 2 hasta la capa 7. Envíe logs a Cortex Data Lake desde Panorama para cortafuegos gestionados, desde cortafuegos individuales (cortafuegos no gestionados por Panorama), desde Prisma Access (anteriormente el servicio en la nube GlobalProtect™), y desde Traps para centralizar y agregar su almacenamiento de logs local y virtual (nube pública y privada) para cortafuegos físicos y VM-Series.
- Utilice API para una integración ajustada con herramientas de defensa de terceros .
- Automatice bucles de retroalimentación que detectan eventos y automatizan respuestas.
    - Etiquete cargas de trabajo y utilice etiquetas como criterios de filtrado para determinar los miembros de grupos de direcciones dinámicas en la política de seguridad. Esto le permite automatizar acciones basadas en eventos de reenvío de logs a un servidor HTTP(S). El evento de reenvío de logs activa la acción al añadir o eliminar de forma dinámica miembros de un grupo de direcciones dinámicas utilizado en la política de seguridad en tiempo real. La política de seguridad determina si los miembros del grupo de direcciones dinámicas tienen permitido o denegado el acceso y el cortafuegos aplica la acción. Por ejemplo, configure un DNS Sinkhole en un perfil de seguridad antispyware para poner en cuarentena automáticamente los sistemas potencialmente comprometidos que intentan acceder al sinkhole. Use etiquetas y reenvío de logs para añadir y eliminar esos sistemas dinámicamente de un grupo de direcciones dinámicas que se adjunta a una regla de política que bloquea y registra todo el tráfico a la dirección del sinkhole. Luego puede investigar sistemas potencialmente comprometidos cuando se lo notifiquen mediante alertas de logs.
    - Utilice Cortex XDR para automatizar el análisis de su red, descubrir comportamientos anómalos que indiquen una posible intrusión y alertar sobre ese comportamiento para que pueda investigar y solucionar el problema. Cortex XDR proporciona visibilidad en el tráfico de red, simplifica la investigación de amenazas al correlacionar logs y le permite identificar la causa raíz de las alertas y responder de inmediato. Utilice las API de Cortext XDR para la integración con Demisto y automatice las respuestas usando los libros de estrategias de respuesta de Demisto que se adaptan a los flujos de trabajo de su empresa, lo que puede reducir el tiempo de respuesta de días a minutos.
    - Utilice WildFire para automatizar el descubrimiento de nuevo malware. Cuando WildFire descubre malware en cualquier parte del mundo, tarda como máximo cinco minutos antes de que WildFire actualice sus perfiles de seguridad para protegerlo contra el nuevo malware.
- Use plantillas y pilas de plantillas en Panorama para automatizar la implementación de políticas.
- Utilice herramientas como Ansible, Terraform y Python para automatizar, orquestar y acelerar la protección de las implementaciones de Prisma Cloud.

Palo Alto Networks le permite diseñar su entorno Zero Trust y aplicar seguridad consistente en todas las ubicaciones:

- Panorama centraliza el control de la política de gestión para múltiples cortafuegos de última generación y aumenta la eficiencia operativa en comparación con la gestión individual de cortafuegos.
- Red corporativa y centro de datos: Utilice cortafuegos de última generación para segmentar la red en microperímetros para sus superficies de protección.
- Nube pública: Use Prisma Access, que usa cortafuegos locales o VM-Series de última generación, y Prisma Cloud (una solución de seguridad de infraestructura de nube basada en API), para implementar la política Zero Trust en entornos de nube. Las nubes privadas virtuales (VPC) definen los límites de protección para segmentar las cargas de trabajo.
- Nube privada: Use cortafuegos VM-Series para implementar la política Zero Trust.
- Sucursales y usuarios móviles: Utilice Prisma Access para proporcionar seguridad basada en la nube y evitar viajes de ida y vuelta a los recursos de la red corporativa. Configure Prisma Access para usuarios y también Prisma Access para redes para proteger sucursales.

  Alternativamente, use un cortafuegos local de última generación con el servicio de suscripción GlobalProtect para extender la política de seguridad y su aplicación a usuarios remotos y sucursales.
- Endpoints: Protección de capa usando el cortafuegos de última generación para la segmentación y la primera capa de protección y usando Traps para la segunda capa de protección. Aplique una política coherente con el uso de VPNs GlobalProtect (instalación local) o Prisma Access (instalado usando

© 2019 Palo Alto Networks, Inc.

Panorama y gestionado para usted en la nube) para ampliar la política a endpoints remotos y permitir que la política se mueva con el usuario. Prisma Access requiere la aplicación GlobalProtect en los endpoints de usuarios móviles. En todos los casos, instale la aplicación GlobalProtect en los endpoints gestionados y utilice GlobalProtect Clientless VPN en endpoints no gestionados (endpoints en los que no puede o no desea colocar un agente, como sistemas asociados o dispositivos personales). Aplique Autenticación múltiples factores cuando sea adecuado para proteger activos de alto valor.

- Aplicaciones SaaS: Utilice Prisma SaaS para escanear, analizar, clasificar y ayudar a proteger las aplicaciones SaaS. Redirija el tráfico de la aplicación SaaS para dispositivos no gestionados a través de su cortafuegos de última generación (el tráfico de los dispositivos gestionados pasa por Prisma Access, GlobalProtect o un cortafuegos de última generación).

Paso 4: Cree la política de Zero Trust

La política de Zero Trust consta de reglas de la lista de permitidos, reglas que permiten que solo los usuarios autorizados accedan a recursos específicos utilizando las aplicaciones especificadas en el momento correcto en los lugares correctos. Si el tráfico no coincide con una regla, el cortafuegos bloquea automáticamente el tráfico. Esto es importante porque:

- Es mucho más fácil conocer las aplicaciones que desea permitir para respaldar su negocio que asumir la tarea interminable de identificar y bloquear todas las aplicaciones que no desea permitir.
- Todas las infracciones y actividades mal intencionadas suceden en las reglas de permiso. Centre la seguridad en el tráfico que permita y permita solo el tráfico requerido para los negocios.

La política de Zero Trust se basa en el Método Kipling. La respuesta a la tupla de 6 preguntas de Rudyard Kipling, "quién, qué, cuándo, dónde, por qué y cómo", le muestra cómo decidir si desea permitir o bloquear el tráfico y cómo crear una política de seguridad que proteja cada superficie de protección. Palo Alto Networks proporciona las capacidades para implementar el Método Kipling en la política de seguridad:

- **¿Quién** debe acceder a un recurso?
  - User-ID identifica a los usuarios y le permite controlar quién accede a un recurso en la política. A través de una lente de mínimo privilegio de acceso (¿quién necesita saber?), permita el acceso solo a individuos, grupos y dispositivos que tengan razones comerciales legítimas para acceder a un recurso.
  - Cree Política de autenticación para verificar las identidades de los usuarios cuando intenten acceder a los recursos. La política de autenticación también determina si se requiere Autenticación de múltiples factores (MFA).
  - Use MFA para proteger servicios y aplicaciones confidenciales al requerir al menos un factor de autenticación adicional además de introducir una contraseña en un Portal cautivo, como un código de un único uso entregado a un teléfono móvil o correo electrónico, antes de que el cortafuegos permita el acceso a servicios, aplicaciones y recursos confidenciales. Para usuarios remotos, configure GlobalProtect para facilitar las notificaciones de MFA (también debe configurar MFA en el cortafuegos).
  - Para los dispositivos que usan GlobalProtect, configure Perfiles de información del host (HIP) para definir la política de acceso para los hosts, aplicar la política en esos hosts y evitar que los dispositivos que no cumplan con sus estándares de seguridad y mantenimiento accedan a los recursos. Por ejemplo, puede usar un HIP para asegurarse de que los endpoints tengan habilitado el cifrado, las firmas antivirus del host estén actualizadas, etc. Si un host no cumple con los requisitos de HIP, la política de seguridad bloquea el acceso.
- **¿Qué aplicación** se utiliza para acceder al recurso?
  - Cree una política de capa 7 basada en aplicaciones utilizando App-ID, que identifica las aplicaciones independientemente del puerto, el protocolo o las tácticas evasivas, para que solo permita las aplicaciones correctas en su red. La política basada en la Capa 3 y la Capa 4 se basa en direcciones IP que un atacante puede suplantar y deja los puertos abiertos a aplicaciones evasivas.

© 2019 Palo Alto Networks, Inc.

- Establezca el servicio en application-default (aplicación predeterminada) para habilitar de forma segura las aplicaciones en sus puertos predeterminados y evite que las aplicaciones evasivas accedan a su red en puertos no estándar.
- Si el cortafuegos ejecuta PAN-OS 9.0 o posterior o un dispositivo Panorama que ejecuta PAN-OS 9.0 o posterior gestiona cortafuegos que ejecutan PAN-OS 8.1 o posterior, utilice Policy Optimizer para examinar las reglas de política existentes (tanto reglas basadas en aplicaciones como reglas basadas en puertos anteriores), identificar reglas no utilizadas e identificar reglas con aplicaciones no utilizadas. Para los cortafuegos que ejecutan versiones anteriores de PAN-OS, utilice Expedition para examinar las reglas de política. (Si necesita migrar una configuración heredada a un dispositivo PAN-OS, siga las Prácticas recomendadas para migrar a una política basada en aplicaciones.

- **¿Cuándo** acceden los usuarios al recurso?

  Para las aplicaciones a las que acceden los usuarios solo durante ciertas horas, aplique un horario [**Objects (Objetos)** > **Schedules (Horarios)** en dispositivos Panorama y cortafuegos] a la regla de política para evitar accesos sospechosos durante las horas de desconexión. Los adversarios a menudo atacan e intentan filtrar datos fuera del horario comercial normal para reducir las posibilidades de ser descubiertos.
- **¿Dónde** se encuentra el recurso?

  Añada la ubicación del recurso de destino a la política. Cuando sea apropiado, también restrinja el origen (zona y dirección IP) del tráfico.
- **¿Por qué** se accede a los datos? ¿Cuál es el valor de los datos si se pierden (toxicidad)?

  Clasifique los datos para comprender su toxicidad: ¿por qué vale la pena proteger los datos? ¿Tendría que revelar la pérdida si un atacante desvelara los datos? Configure el filtrado de datos para evitar que la información confidencial salga de su red y use herramientas de clasificación de datos para proporcionar metadatos sobre los datos. Comprender la toxicidad de los datos le ayuda a determinar cómo proteger los datos, qué hacer con los datos después de usarlos y cómo etiquetarlos para usarlos en la política.
- **¿Cómo** debe permitir el acceso al recurso?

  Aplique Content-ID y las prácticas recomendadas para protegerse contra las amenazas en el tráfico de aplicaciones:

  - Aplique la filosofía de mínimo privilegio de acceso a la política de seguridad. Permita que solo los usuarios con motivos comerciales legítimos accedan solo a las aplicaciones a las que necesitan acceder con fines comerciales solo en el momento adecuado y solo de la manera adecuada.
  - Registre todo el tráfico interno y externo a través de la Capa 7. Las reglas de política de cortafuegos habilitan la creación de logs de forma predeterminada. Reenvíe logs a Cortex Data Lake (o a Panorama o los Recopiladores de logs) para consolidar los logs para un análisis más fácil y completo.
  - Aplique políticas y prevención de amenazas de manera consistente en todas las ubicaciones (red, nube, endpoints), para todos los usuarios locales y remotos, de modo que la política siga al usuario donde quiera que vaya, para todas las aplicaciones y para todos los recursos. Una política incoherente aumenta las vulnerabilidades, es difícil de entender y mantener, y puede afectar negativamente los requisitos de cumplimiento y las auditorías. Use cortafuegos físicos de última generación y cortafuegos virtuales VM-Series como gateways de segmentación para aplicar una política coherente de Zero Trust, capa 7 y método Kipling en la red y la nube. Utilice Prisma Access (nube) y GlobalProtect (instalación local y con Prisma Access) para extender la política coherente de Zero Trust a los endpoints. Para endpoints no gestionados (endpoints en los que no desea colocar o no puede colocar un agente), use GlobalProtect Clientless VPN para aplicar una política coherente. Cree y reutilice plantillas y pilas de Panorama para aplicar una política coherente en ubicaciones similares, como sus centros de datos o sus perímetros.
  - Configure perfiles de seguridad (Perfiles de protección frente a vulnerabilidades para IPS, antivirus y WildFire para proteger contra malware, incluido el malware de día 1, perfiles antispyware para evitar amenazas de tipo comando y control, perfiles de bloqueo de archivos para bloquear o alertar sobre tipos de archivos peligrosos, y Filtrado de URL para controlar el acceso a sitios web, ayudar a prevenir ataques de phishing e imponer la búsqueda segura para motores de búsqueda) y aplicarlos a todo

© 2019 Palo Alto Networks, Inc.

el tráfico permitido. Siga las prácticas recomendadas para los perfiles de seguridad cortafuegos del centro de datos y cortafuegos perimetrales.

- Utilice Prácticas recomendadas de WildFire para detectar y prevenir el malware de día cero.
- Utilice las Prácticas recomendadas de descifrado para descifrar tanto tráfico como las regulaciones y los requisitos comerciales le permitan descifrar para poder inspeccionar la mayor cantidad de tráfico posible. No puede proteger la red de amenazas que no puede ver.
- Utilice el Servicio DNS Security para proporcionar acceso en tiempo real infinitamente escalable a las firmas DNS, análisis en tiempo real de las solicitudes DNS y firmas DNS avanzadas generadas mediante aprendizaje automático y análisis predictivo.
- Como también incluye el determinar qué hacer con los datos confidenciales después de usarlos: extráigalos utilizando cifrado, tokenización o enmascaramiento, o deshágase de ellos mediante su eliminación o archivado. Archive datos obsoletos (aproximadamente el 80% de los datos en la mayoría de los sistemas no se han usado en dos o más años).
- Utilice Cortex XDR para refinar y mejorar la política.

El Método Kipling le permite crear una política de seguridad que defiende cada superficie de protección de manera adecuada porque le lleva a comprender quién debe tener acceso, cómo deben acceder a ella, cuándo deben acceder a ella y las protecciones que se deben aplicar. Puede desarrollar reglas de política a través del desarrollo de declaraciones comerciales basadas en el Método Kipling. Por ejemplo:

	Quién	Qué	Cuándo	Dónde	Por qué	Cómo
Método	User-ID	App-ID	Límites de tiempo	Objeto del sistema	Clasificación	Content-ID
Local	Epic_Users	Epic	Cualquier momento	Epic_Srvr	Tóxico (los datos tienen un alto valor)	Descifrar, inspeccionar (perfiles de seguridad), registrar el tráfico
Nube	Ventas	Salesforce	Horas de oficina	Estados Unidos	Tóxico (los datos tienen un alto valor)	Descifrar, inspeccionar (perfiles de seguridad), registrar el tráfico

En ambos casos, el cortafuegos solo permite el tráfico que satisface todas las condiciones en la tupla de Kipling y pasa la inspección. El cortafuegos automáticamente deniega todo el tráfico que no coincide con una regla permitir.

Además de la política de seguridad, autenticación y descifrado, utilice las Prácticas recomendadas para DoS y la protección de zona para proteger servidores vitales de ataques de denegación de servicio (DoS).

Para los cortafuegos que aún no ha configurado, use plantillas de configuración IronSkillet de día 1 para implementar una política de prácticas recomendadas del Día 1, luego ajuste la política para que se adapte mejor a sus superficies de protección.

Paso 5: Supervise y mantenga la red

La seguridad es un proceso iterativo porque la creación de logs y la supervisión revelan mejoras a realizar y porque su negocio y su red cambian con el tiempo. Siga los procesos operativos que desarrolló al diseñar la red para mantener y actualizar continuamente los controles de prevención.

© 2019 Palo Alto Networks, Inc.

- Descifre, inspeccione y registre todo el tráfico (interno y externo) a través de la Capa 7.
- Reenvíe logs a Cortex Data Lake desde Panorama para cortafuegos gestionados, desde cortafuegos individuales (cortafuegos no gestionados por Panorama), desde Prisma Access y desde Traps para centralizar y agregar su almacenamiento de logs local y virtual (nube pública y privada). Esto proporciona visibilidad sobre el tráfico de su red y las superficies de protección.
- Actualice la política y posiblemente añada nuevas superficies de protección basadas en la inteligencia de Cortex XDR, que utiliza los datos de Cortex Data Lake y el aprendizaje automático para automatizar el análisis de su red en función del comportamiento normal de su red e para identificar comportamientos anómalos que pueden indicar una intrusión u otra amenaza. La actividad de amenazas que se centra en elementos DAAS que no están en una superficie de protección puede resaltar las superficies de protección que usted no tuvo en cuenta cuando originalmente definió sus superficies de protección.
- Use Cortex XDR para obtener visibilidad sobre el tráfico de su red, simplificar la investigación de amenazas al correlacionar logs y permitir la identificación de la causa raíz de las alertas y responder de inmediato.
- Utilice las API de Cortext XDR para la integración con Demisto y automatice las respuestas usando los libros de estrategias de respuesta de Demisto que se adaptan a los flujos de trabajo de su empresa, lo que puede reducir el tiempo de respuesta de días a minutos.
- Utilice Prisma Cloud para juntar y proporcionar visibilidad de los datos de configuración, la información de actividad del usuario y la información de tráfico de la red. Prisma Cloud analiza los datos y proporciona información concisa y procesable.
- Siga las Prácticas recomendadas para actualizaciones de contenido de aplicaciones y amenazas para obtener las App-ID nuevas y modificadas y mantener sus firmas de amenazas actualizadas.
- Use la Herramienta de evaluación de prácticas recomendadas para medir el progreso hacia una configuración de prácticas recomendadas y para ayudarle en la transición a una estrategia de seguridad de prácticas recomendadas .
- Supervise la actividad de red, utilice informes predefinidos y genere informes personalizados para obtener visibilidad de su entorno.
- Mantenga unido al equipo multifuncional para ayudarle a mantener su implementación de Zero Trust a medida que la red y el negocio evolucionan, y cree educación y formación para garantizar que los nuevos miembros del equipo entiendan la estrategia y la implementación.
- Continúe automatizando acciones y respuestas a medida que avanzan las capacidades de automatización.

© 2019 Palo Alto Networks, Inc.

Recursos de Zero Trust

La siguiente documentación técnica, notas del producto, transmisiones web, vídeos y otros recursos proporcionan más información y contexto para su estrategia Zero Trust. Además de la información en este documento y los recursos enumerados, puede realizar una consulta al equipo de expertos de los Servicios profesionales de Palo Alto Networks, quienes le ayudarán a diseñar e implementar su estrategia Zero Trust.

- How to Build a Zero Trust Network (Cómo desarrollar una red de Zero Trust)(transmisión web a petición)
- Debunk the Myth Around Implementing Zero Trust(Desacreditar el mito sobre la implementación de Zero Trust) (transmisión web a petición)
- Descripción general de Zero Trust
- Zero Trust (página web de Zero Trust de Palo Alto Networks)
- Prácticas recomendadas para ejecutar en Zero Trust (hoja de ruta de transformación)
- Simplificación de la implementación de Zero Trust utilizando una metodología de cinco pasos (documento técnico)
- Proteja la nube: Seguridad en la nube con Zero Trust
- Zero Trust Cloud Security (vídeo)
- La verdad sobre Zero Trust (infografía)

Documentación técnica de Palo Alto Networks

Transición a las Prácticas recomendadas:

- Introducción a la BPA
- How to Run a BPA (Cómo ejecutar una BPA) (vídeo)
- Understanding BPA Results (Cómo interpretar los resultados de una BPA) (vídeo)
- Página de evaluación de prácticas recomendadas de la comunidad en directo

Portal de documentación de prácticas recomendadas:

- Introducción a las prácticas recomendadas
- Política de seguridad recomendada de la puerta de enlace de Internet
- Política de seguridad recomendada para el centro de datos
- Prácticas recomendadas para migrar a una política basada en aplicaciones
- Prácticas recomendadas para proteger el acceso administrativo
- Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas
- Prácticas recomendadas de descifrado
- Prácticas recomendadas de protección DoS y de zonas
- Prácticas recomendadas de la implementación de WildFire

Expedition

IronSkillet (Plantillas de configuración del Día 1)

Servicio de atención al cliente

Evaluación de la postura de prevención (evaluación consultiva complementaria de sus capacidades de prevención)

Palo Alto Networks NextWave Technology Partners

© 2019 Palo Alto Networks, Inc.