REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

RedShift Networks UCTM vs. Firewall Con Capacidad De VoIP

Datos Generales

RedShift Networks es líder en el Manejo de Amenazas de Comunicaciones Unificadas (UCTM). Somos los primeros en la industria en ofrecer soluciones de seguridad integrales para redes, sistemas y aplicaciones de Voz por IP, Video, Comunicación Unificada y Colaboración. Nuestro equipo central se encuentra integrado por ejecutivos de primer nivel de empresas líder en sistemas y comunicaciones tales como Avaya, Cisco, SGI, Alcatel-Lucent, HP, Secure Computing y Ascend. Nuestro panel de asesores incluye líderes del mundo de la tecnología y del mundo académico. Fundada en 2006, RedShift Networks tiene su base de operaciones en Silicon Valley, California y cuenta con oficinas en la India. Visite www.redshiftnetworks.com.

"Redshift, Nombrado 4to. Lugar en Negocios Emergentes'" — por Yankee Group, Líder en Análisis IT

El Mercado Actual de Comunicación Unificada

El Mercado de Comunicación Unificada y Colaboración actualmente crece de manera muy veloz en empresas globales como Cisco, Microsoft, IBM, Avaya, Polycom, HP, Siemens, Alcatel y Google, quienes aprovechan el poder de las nuevas habilidades de interconexión del mundo de IP para la unificación de redes tradicionales de voz, video e información con los poderosos servicios de VoIP/CU que ahora se ofrecen. Por esta razón, la antigua definición de perímetro de seguridad ya no aplica. Asimismo, con la creación de nuevas y poderosas tecnologías de telefonía fija y móvil como lo son el IPad, el Android, el Smartphone, etc., los clientes entienden la necesidad de servicios para VoIP/CU como nunca antes. Por lo anterior, es indispensable proteger las redes, aplicaciones y sistemas del embate de nuevas amenazas, ataques y vulnerabilidades. Con el aumento de redes complejas, terminales y hábitos de usuario, es fundamental tener el completo control y visibilidad de las redes de CU así como cumplir con los reglamentos vigentes en la industria.

El mundo de Comunicación Unificada y Colaboración se centra alrededor de comunicaciones en tiempo real como son: VoIP, Conferencias en Video,

Comunicación Unificada y Colaboración

« Una Nueva Era en Amenazas »

En 2008, ataques aumentaron en un 48%. Todos hemos escuchado acerca de los hackers, virus, SPAM y otros tipos de ciber-ataques a redes de información, así como los millones de dólares en pérdidas que generan.

Una nueva gama de amenazas y ataques que afectan a redes de VoIP, Video y CU y C, se suman a los ataques a redes de información ya existentes

POR QUÉ EMPRESAS AHORA DESPLIEGAN REDSHIFT MACU

- Incremento al tiempo efectivo de funcionamiento debido a las mejoras en monitoreo y a la eliminación de amenazas a VoIP/CU
- Cumplimiento con requerimientos de seguridad y reglamentación
- Prevención de daño al prestigio e imagen de las empresas
- Asegura continuidad en los negocios
- Ofrece servicios de seguridad de vanguardia a clientes importantes con necesidades críticas de seguridad
- Ofrece asesoría de seguridad para una comunicación confiable y unificada
- Punto único de control de funciones de seguridad y protección para clientes de CU

RedShift Networks UCTM vs. Firewall Con Capacidad De VoIP

Mensajería Unificada, aplicaciones de Centro de Contactos/Llamadas, Sistemas IVR y ACD, Tele Presencia, Colaboración, y muchas otras aplicaciones de comunicación. Algunos analistas han calculado que para el año 2013, el mercado sumará los $35 mil millones de dólares. Otros predicen crecimientos aún mayores dada la tendencia de empresas globales a utilizar estas tecnologías cada vez más frecuentemente. RedShift Unified Communication and Collaboration Networks: un mercado de $35 mil millones de dólares para el año 2013

Ataques a Seguridad de CU y C

en los últimos 12 meses:

- *Mayo 11, 2010 – FBI alerta Ataques a Telefonía de IPs*
- *Abril 14, 2010 –Ataques de Fuerza Bruta Amazon EC2 SIP*
- *Dic. 17, 2009 – Predator Drone Hackeado (Videoalimentación)*
- *Octubre 23, 2009 – Auriculares Polycom VOIP Vulnerables*
- *Octubre 20, 2009 – Correo de Voz deGoogle Expuesto*

GARTNER (2007) Empresas que no inviertan hoy en Seguridad de Telefonía IP, terminarán gastando 20% de su presupuesto de Operaciones de Seguridad de 2011 en este rubro

Comunicación Unificada y Colaboración

« Limitantes del Firewall Next Gen»

- » No genera análisis e inspección exhaustivos de estados de llamadas de CU y C
- » No ofrece conocimiento de aplicación de servicios
- » No ofrece defensa de Cero Días para CU y C
- » No ofrece administración detallada de reportes de llamadas o incidentes para CU y C
- » Alto porcentaje de resultados Falso-Positivos similares a solu- ci ones de seguridad de datos (ej: IDS/IPS)
- » No ofrece análisis de comportamiento de CU y C
- » No ofrece rastreo ni bloqueo en tiempo real de flujo de CU y C
- » Sin Integración de Infraestructura

Firewall con capacidad de VoIP

Los Firewalls de información tradicionales tales como dispositivos Checkpoint UTM y NetScreen, actualmente empiezan a incorporar capacidades de procesamiento de VoIP a su arquitectura UTM básica. Los Firewalls UTM no son la mejor opción en soluciones de seguridad dado que tienden a combinar múltiples soluciones de seguridad sin una correlación profunda entre estados y sin defensa a profundidad. El protocolo de procesos de VoIP de estas soluciones por lo general realiza validación de sintáxis limitada. Las arquitecturas actuales de seguridad de información no cuentan con la capacidad adecuada para manejar aplicaciones tales como flujos de Voz por IP, Medios, Comunicación Unificada o Colaboración.

Lo que puede ofrecer un Firewall con Capacidad de VoIP:

- » Crea aplicaciones de información y protocolos resistentes a generación de falso-positivos
- » Visibilidad y Control de Aplicaciones, Usuarios y Contenidos que se adhieran a las políticas empresariales
- » Combina aplicaciones, usuarios e información que identifiquen específicamente a una aplicación, usuario o tipo de contenido
- » El grado de inspección por lo general se limita a unos cuantos tipos de encabezados de paquetes
- » Su estrategia yace en permitir o bloquear ciertos tipos de aplicaciones o usuarios
- » Protege contra virus, spyware, gusanos, amenazas/vulnerabilidades de información por medio de firmas
- » Protección limitada para algunas pruebas de anomalías de protocolos
- » Reglamentos básicos de saneamiento de tráfico de red utilizando filtros URL

RedShift Networks UCTM vs. Firewall Con Capacidad De VoIP

Lo que no puede ofrecer un Firewall con Capacidad de VoIP:

- No soporta estados complejos de comunicación CU y C. Es un requerimiento para poder ofrecer Control, Visibilidad y Protección a redes, aplicaciones y terminales de CU y C
- No administra ni finaliza llamadas de CU y C – parte de la función de un B2BUA. Por lo anterior, no reconoce la señalización profunda, los medios, ni los estados de CU
- Sólo reconoce SIP, SCCP o el paquete H.323 como un paquete de aplicación (ejemplo: Avaya Communication Manager, Cisco Call Manager, etc.)
- No ofrece protección 0-Day contra miles de amenazas y vulnerabilidades de seguridad de CU y C (ejemplo: Ataques a Protocolos de CU/VoIP por Fuzzing , Fraude Telefónico, SPIT, Amenazas a Medios, Ataques de Voz/UC DOS, War Dialing, Secuestro de Presencia, Información ⇨ Amenazas de Voz, etc.)
- No ofrece soporte para ACL ni manejo de incidentes
- Las pruebas de anomalías de protocolo están limitadas a sólo algunas implementaciones de RFC
- No rastrea los servicios de CU ya que esto requiere de correlaciones más profundas
- Los Firewalls de información generan grandes cantidades de Falso-Positivos
- No ofrece un análisis detallado de tráfico de llamadas de CU (ejemplo: procesamiento detallado de llamadas de CU, reportes, estados activos, historial de llamadas, anomalías de usuarios, etc.)
- No reporta estadísticas de tráfico de medios
- No audita detalladamente todos los estados de sesiones de VoIP/CU, puntos terminales, ni hábitos de usuario
- No se integra con la infraestructura de CU y C (ejemplo: IP PBX, conferencias, colaboración, presencia, mensajes unificados, centros de llamadas, etc.)
- No rastrea ni bloquea en tiempo real el tráfico de CU no regulado

BENEFICIOS Y VENTAJAS DE SOLUCIONES DE REDSHIFT UCTM

- Fácil Despliegue
- 100% QoS
- Confiablididad Five- 9
- Baja Sobrecarga por Latencia
- Falso- Positivos casi nulos
- Falso-Negativos casi nulos
- Alta correlación entre llamadas y estados de aplicación CU
- Soporte completo de comunicaciones en tiempo real
- Soporte completo de red heterogénea compleja

Soluciones de RedShift Networks

Los productos de seguridad de información tales como Anti_SPAM, Virus y IDS/IPS han generado un mercado millonario en los últimos 4-5 años. CU y C enfrenta un nuevo problema de seguridad.
RedShift Networks ha creado una plataforma de tecnología única de Flujo Sincronizado Proactivo de Alto Rendimiento la cual ofrece seguridad exhaustiva para redes de CU y C. La tecnología central de detección es única, utilizando varios motores proactivos de protocolo neutral que ejecutan un manejo profundo de estados de llamadas de VoIP y CU, y de correlación y detección de cumplimiento de regulaciones. Se han registrado cuatro patentes.

RedShift Networks
4000 Executive Parkway — Suite 290 — San Ramon, CA 94583 — USA
Phone +1 925 272 0100 +1 866 824 5775 (toll free) www.redshiftnetworks.com info@redshiftnetworks.com

RedShift Networks UCTM vs. Firewall Con Capacidad De VoIP

Requerimientos De Seguridad De CU&C

Necesidades de Seguridad de CU & C	Firewall	UCTM
CU/VoIP	Limitado (VoIP)	Si (VoIP/cu)
Amenazas a Infraestructura IP/TCP	Si	Si
Ataques a Voz/Video/CU DOS/DDOS — Ataques por Inundación, Ataques Stealth	Limitado (voz solamente)	Yes (stealth/voz/vi/deo/cu)
Prevención de Spoofing — Call-ID spoofing, Phishing de voz, spoofing de Presencia, Robo de Identidad	No	Si
Ataques de SPAM de Voz/Video/CU	No	Si
Firewall de Señalización — fraude Telefónico, Fuzzing, ...	No	Si
Laboratorios y Firmas de Vulnerabilidades de CU/VoIP	Parcial	Si (Condor)
Control de Aplicaciones de CU	Parcial	Si
Politicas de Reasignación de Rutas/ Control de Admisiones	No	Si
Revisión de Integridad de Mensajes (SDP, HTTP, XMPP)	No	Si
Firewall de Medios — Secuestro, DOS	No	Si
Señalización/Codificación de Medios (SIP/TLS, SRTP)	No	Si
Seguridad de Trinking SIP — DPI	No	Si
Cumplimiento Regulación / Privacidad	Parcial	Si
Validación de Datos — Datos ←→ Amenazas a Voz	Si	Si
Controles AAA con recononcimiento VoIP/CU	No	Si
Amenazas a Aplicaciones e Infraestructura de CU	No	Si