REDSHIFT
NETWORKS
Secure Cloud Communication and Collaboration.

Manejo de Amenazas A Comunicación Unificada (UCTM)

Comunicación y Colaboración Segura

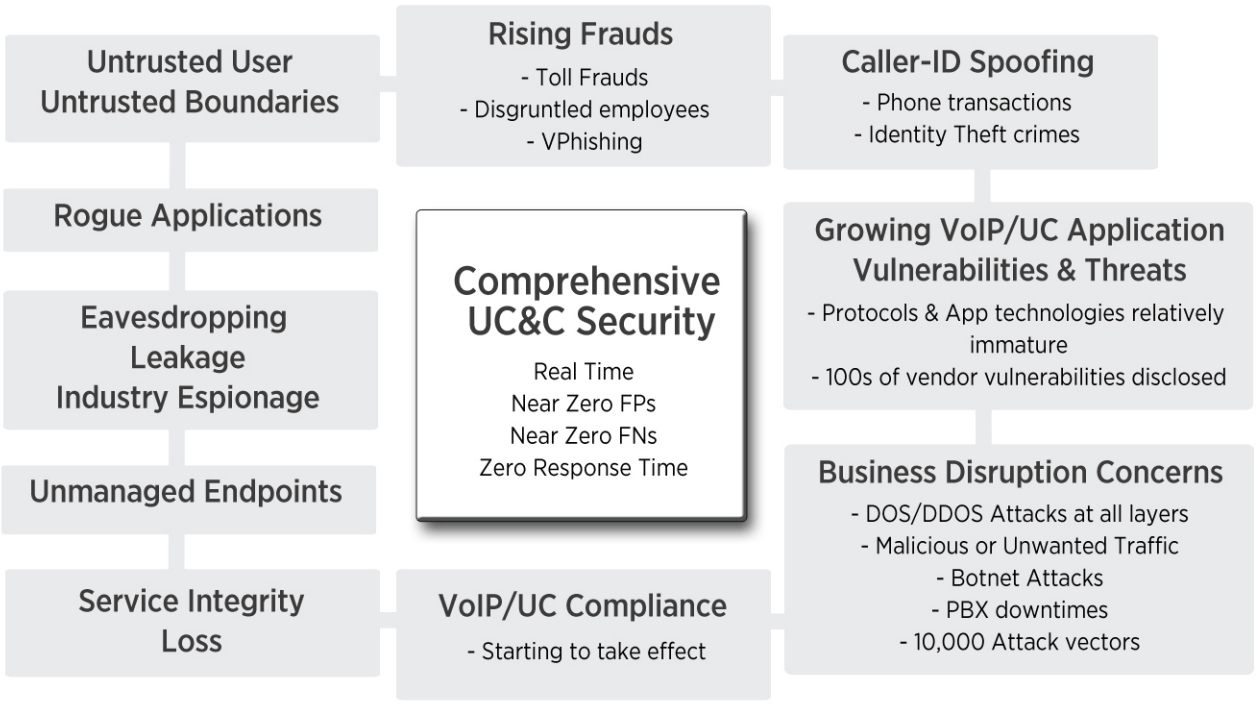
Secure Cloud Communication and Collaboration.

Manejo de Amenazas
A Comunicación Unificada (UCTM)
Comunicación y Colaboración Segura

Información General

El surgimiento de tecnologías de Comunicación Unificada, Colaboración y Voz por IP y Video está generando un cambio fundamental en la industria de la tecnología. Sistemas tradicionales de comunicación y aplicaciones que corren en redes TDM están siendo sustituidas rápidamente por sus contrapartes de IP, lo cual genera numerosos beneficios para las empresas. Los beneficios obtenidos incluyen bajos costos de operación, la habilidad de obtener servicios de comunicación habilitados por software, tener facilidad de administración, fácil uso y adaptabilidad a los cambios y fluctuaciones en los negocios y a su vez la facilidad trabajar utilizando estándares abiertos.

Quienes venden soluciones de CU están unificando las operaciones de aplicaciones de datos (y de servicios de CU) con las características particulares de telefonía IP. Este hecho aumenta significativamente la conectividad entre empleados y la productividad de los negocios. La combinación actual de estos mundos se llama “Comunicación Unificada” (CU) cuando la integración sucede desde la terminal o PC del usuario final, y “Proceso de Negocios con Comunicación Habilitada” cuando la integración ocurre con una aplicación empresarial que corre en servidores dedicados. Como resultado de lo anterior, ahora es posible contar con amplios servicios desde cualquier punto, a cualquier hora y desde cualquier dispositivo ya que los servicios de comunicación CU tales como Presencia y Colaboración ahora se pueden ofrecer desde cualquier dispositivo habilitado con IP.



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

Manejo de Amenazas A Comunicación Unificada (UCTM)

Comunicación y Colaboración Segura

Es importante comprender que si bien las redes y aplicaciones de Comunicación Unificada, Colaboración, Voz por IP y Video prometen grandes ventajas, sus requerimientos y riesgos de seguridad son diferentes a los que se presentan en aplicaciones y redes de datos convencionales. La naturaleza de las comunicaciones en tiempo real sumada a la complejidad de interconexión entre varios elementos, genera que los riesgos a la seguridad y los vectores de amenaza sean alarmantemente altos.

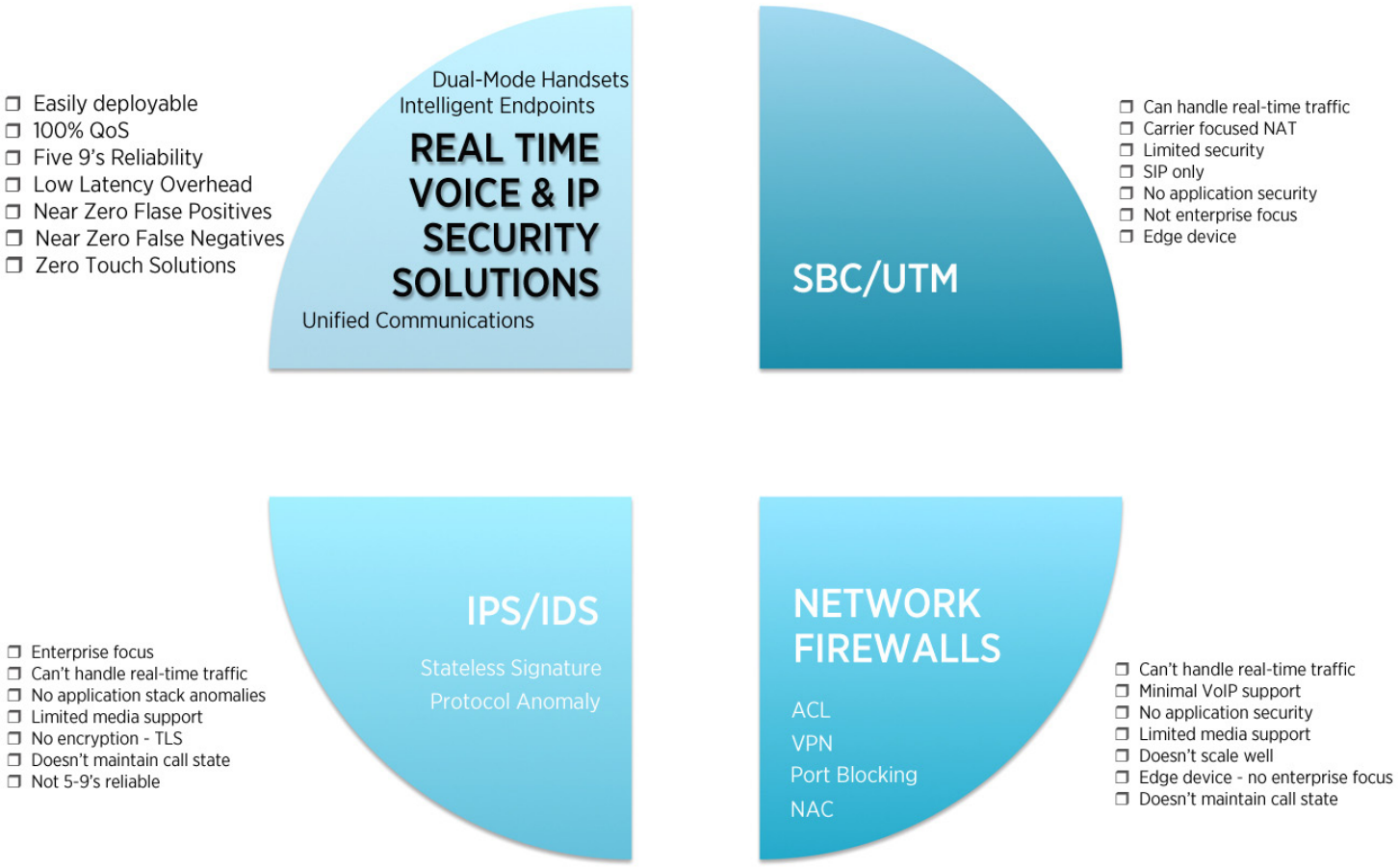
La figura de arriba presenta un resumen de los posibles riesgos que deben evaluarse antes de desplegar ambientes masivos. La protección que ofrecemos abarca desde mecanismos de detección de fraudes en tiempo real, manejo de vulnerabilidades, control de aplicaciones y usuarios maliciosos, cumplimiento con regulaciones, manejo de amenazas a infraestructura y aplicaciones tales como ataques VDOS/UC-DOS, ataques de SPAM a telefonía por Internet (SPIT), espionaje, Spoofing, recolección indebida de números, anomalías de protocolos, ataques por Fuzzing, amenazas a señalización/medios, fraude telefónico, etc.

El Manejo de Amenazas a Comunicación Unificada (UCTM) se encuentra dentro de una nueva categoría de productos. Es una solución altamente especializada y diseñada para ofrecer completa protección, visibilidad y control de tráfico de IP – voz, medios, comunicación unificada y colaboración. La solución ofrece un enfoque combinado hacia la seguridad que incluye herramientas ya utilizadas tales como inspección de estados, detección de anomalías de protocolos y prevención de intrusiones aplicada a protocolos de VoIP y CU, pero también técnicas muy sofisticadas de correlación y conocimiento/aprendizaje de aplicaciones y usuarios que juntas ofrecen soluciones integrales de seguridad. Las herramientas de MACU combinan servicios separados de seguridad tradicionales dentro de un dispositivo único, el cual proporciona completo control, visibilidad y protección a infraestructuras centrales, servidores, usuarios y aplicaciones de comunicación unificada y colaboración.

¿Por qué necesita usted UCTM?

Las aplicaciones de datos se encuentran debidamente administradas y aseguradas por las prácticas de seguridad y administración de datos actuales. Estas soluciones de seguridad basadas en información por lo general cumplen con las necesidades de administradores de redes. Sin embargo, con la reciente integración de aplicaciones de comunicación con características de voz, medios y comunicación unificada, nuevas vulnerabilidades y amenazas empiezan a surgir que no se conocían anteriormente. Redes de comunicación que antes se encontraban virtual o físicamente separadas del resto de la red ahora se encuentran expuestas a innumerables cuestiones relacionadas con la convergencia de información y datos. Administradores de redes y seguridad requieren de nuevas herramientas para tratar con la confiabilidad y disponibilidad de bienes empresariales, infraestructura y puntos terminales de servicios de comunicación unificada.

Se identifican cinco propiedades específicas para que cualquier solución maneje adecuadamente los requerimientos de seguridad de VoIP y CU así como los desafíos de despliegue:



Categoría I: Requerimientos de Tiempo Real

- La confiabilidad de 5-9 genera solo 5 minutos de tiempo de inactividad por año
- Baja latencia para señalización y medios
- Requerimientos estrictos de variación de retardo en calidad de servicio (QoS)
  - 100 µs para Medios
  - 2 mSec para Señalización

Categoría II: Requerimientos de Seguridad

- Baja tolerancia a Falso-Positivos
- Baja tolerancia a Falso-Negativos
- No se permite el re-intento de llamadas
- Procesos de tráfico codificados (SIP/TLS, SRTP)

Categoría III: Requerimientos de Tecnología

- Capacidad de inspección de paquetes de tráfico VoIP-CU de Layer3 – Layer7
- Arquitectura heterogénea que abarca elementos de solución proactivos y reactivos
- Soluciona la necesidad de tener niveles múltiples de estados de llamadas con capacidad de aprendizaje adaptado tanto de aplicaciones de CU, cómo de puntos terminales de VoIP
- Correlación avanzada entre estados de protocolo e incidentes de seguridad abarcando diferentes niveles y módulos de seguridad

Manejo de Amenazas
A Comunicación Unificada (UCTM)
Comunicación y Colaboración Segura

» Trato exhaustivo de amenazas de seguridad a aplicaciones de VoIP, CU y CEBP
  • Detección de anomalías de protocolo SIP/SCCP/H.323, prevención de SPIT, IPS, y voz DOS, espionaje, fraude telefónico, recolección indebida de números, ataques MITM, etc.
» Sistema de administración de incidentes y conocimiento de políticas de CU

Categoría IV: Enfoque Carrier

» Requerimientos de interoperabilidad más profundizados con sistemas dispares
» Servicios complejos que abarcan múltiples protocolos
» Solución única de seguridad – no es una combinación de soluciones separadas
» Despliegue Zero-touch

Categoría V: Enfoque hacia Comunicación de CU y CEBP

» Fuerte integración con IP-PBX y otros elementos de infraestructura – fácil de desplegar y administrar
» Fácil integración con soluciones de terceros ofreciendo servicios de CU y SOA (ejemplo: Microsoft, SAP, BEA, IBM)
» Ofrece visibilidad de todo el tráfico de VoIP y CU
» Ofrece control para todos los servicios, aplicaciones y bienes de CU

Soluciones de Seguridad Actuales:

1. Vendedores IDS/IPS – Son efectivos en enfoque empresarial (Categoría IV) pero no tienen la capacidad adecuada para cubrir los requerimientos de comunicación en tiempo real (Categoría I). Generan grandes cantidades de falso-positivos (Categoría II) y carecen de los elementos de tecnología (ejemplo: correlación avanzada de estados de llamadas) necesarios para tratar las complejas amenazas que existen contra protocolos de VoIP múltiples (Categoría III). Las soluciones convencionales de seguridad de datos también carecen de un enfoque real hacia comunicación de CU y CEBP (Categoría V).

2. Vendedores de UTM – Las propiedades de estas soluciones son muy similares a las de IDS/IPS, pero carecen de elementos tecnológicos y de solución que sean los mejores en su clase. Cuentan con precios significativamente más bajos y están enfocados hacia empresas pequeñas y medianas. Los dispositivos UTM presentan grandes fallas en aspectos de rendimiento. No abordan – Categorías II, III y V.

3. Vendedores SBC – Soluciones SBC son muy capaces en la Categoría I (tiempo real) y ofrecen una seguridad aceptable para despliegues de implementaciones con proveedores de servicio y perimetrales. Sin embargo, no se encuentran enfocados hacia empresas y carecen de los elementos de tecnología y soluciones requeridos para ofrecer seguridad adecuada a aplicaciones de CU y CEBP (ejemplo: Categorías III, IV y V).

4. IP PBX actuales – Principalmente enfocados a ofrecer soluciones y equipos de voz a usuarios finales. Son efectivos en tiempo real y se enfocan a empresas y CU. (Categorías I, IV y V). Sin embargo, ofrecer soluciones de seguridad no es su objetivo principal. (Categorías II y III).

En resumen, las soluciones de seguridad convencionales tales como IDS/IPS appliances, firewalls de información y vendedores de UTM y/o SBC no cuentan con la capacidad suficiente para afrontar los complejos requerimientos y retos de seguridad y despliegue que requieren las aplicaciones de VoIP y CU.

Las Crecientes Amenazas y Vulnerabilidades

Los investigadores de RedShift Networks han analizado miles de amenazas provenientes de varias fuentes como lo son VOIPSA Group, CERT, BugTraq además de otras vulnerabilidades publicadas por varios vendedores IP-PBX.

VoIP Fuzzing	Malformed Request (Protocol Fuzzing)	Malformed Protocol Messages	PROTOS Suite	Condenomicon Suite	Spirent ThreatEx	MuSecurity
Eavesdropping	Call Pattern Tracking	Number Harvesting	Conversation Eavesdropping and Analysis	Voicemail Reconstruction	TFTP Configuration File Sniffing	Conversation Reconstruction
VoIP Interception/ Modification	Call Blackholing	Conversation Alteration	Conversation Degrading	Conversation Hijacking	False Caller Identification	DTMF Alteration/ Recording
Service Abuse/ Integrity	Call Conference Abuse	Call Stealing (Toll Fraud)	Identity Theft	Registration Spoofing/Attacks	Misconfiguration of Endpoints	Premium Rate Service Fraud
Flood based Diruption of Service	Registration Flooding	User Call Flooding	Directory Service Flooding	DoS on Signaling	RTP DoS Attacks	Distributed DoS Attacks
Signaling or Media Manipulation	Fake Call Teardown Messages	Call Hijacking	Registration Removal/ Hijacking/ Addition	Wiretapping	SPIT	Key Logging/ DTMF Logging
OS Vulnerabilities	Cisco Call Manager Vulnerabilities	Avaya Communications Manager	Microsoft LCS/ OCS Server	Nortel	Alcatel Lucent	Siemens/NEC
VoIP Scanning & Enumeration Tools	Nessus	SIP-Scan	SIPp	Sivus	iWAR	SIPCrack
Data Threats	SQL Injection	Cross-Site Scripting	Malware	Viruses	Web Vulnerabilities	Buffer Overflows
UC Application Threats	UM - Message Waiting Indication (MWI) Attacks	UM - Manipulation of User Mailbox	UM - VoiceMail Retreval Threats	UM - QoS Degradation	Conference - Illegal Join/ Leave Conference Attacks	Conference - Moderation Functions Attacks

Manejo de Amenazas A Comunicación Unificada (UCTM)

Comunicación y Colaboración Segura

Las conclusiones observadas indican que los despliegues de VoIP y CU presentan una gran variedad de amenazas a partir de diferentes puntos de entrada y vectores de ataque. Estos abarcan desde la explotación de debilidades en los niveles de redes, puntos terminales infectados con malware, vulnerabilidades OS, vulnerabilidades en la implementación de protocolos, ataques de rechazo de servicio por voz y SPIT, ataques a los niveles de aplicaciones de CU y/o debilidades de configuración de dispositivos.

La tabla de arriba presenta las categorías más Importantes de vectores de amenaza, múltiples ataques específicos reportados, las herramientas de uso público utilizadas, así como otra información publicada en varios artículos.

1. Vendedores IDS/IPS – Ofrece buena protección reactiva ante amenazas de información y vulnerabilidades de OS a través de soporte por firmas. No ofrece protección proactiva. No ofrece protección contra las demás categorías ni contra amenazas combinadas que afecten elementos de información y voz, por ejemplo: secuencias click-2-.call generadas desde un buscador.

2. Vendedores UTM – Ofrece protección menos efectiva que IDS/IPS

3. Vendedores SBC – Soluciones SBC son muy capaces en la Categoría I (tiempo real) y ofrecen una seguridad aceptable para despliegues de implementaciones con proveedores de servicio y perimetrales. Sin embargo, no se encuentran enfocados hacia empresas y carecen de los elementos de tecnología y soluciones requeridos para ofrecer seguridad adecuada a aplicaciones de CU y CEBP (ejemplo: Categorías III, IV y V).

4. IP PBX actuales – Solamente ofrecen seguridad básica de manejo y aplicación de políticas.

Comunicación y Colaboración Segura

Para tratar con los crecientes problemas y retos de seguridad, RedShift Networks ha creado una línea de productos que ofrece:

1. “Proteccion” a través de un híbrido de identificación de amenazas estáticas aunado a un motor de aprendizaje adaptable y dinámico que identifica tráfico anormal en tiempo real.

2. “Visibilidad” por medio del análisis y reporte de sesiones y tráfico de redes de VoIP, CU y CEBP.

3. “Control” a través de un motor configurable de Aplicación de Políticas que permite que los administradores de IT aplacen, bloqueen o aceleren el tráfico que consideren indeseable.

RedShift Networks logra lo anterior sin sacrificar el desempeño ni la productividad de los empleados. RedShift Security Appliances ofrecen un punto de integración, visibilidad, control y protección para Comunicación Unificada Empresarial.

Manejo de Amenazas
A Comunicación Unificada (UCTM)
Comunicación y Colaboración Segura

RSN – Línea de Productos “Hawk/Eagle/Falcon”

- ✓ Synchronous Flow Security Technology TM
- ✓ Protegido por Patentes....
- ✓ Tecnología dinámica de real-stream
- ✓ Arquitectura proactiva de evaluación de amenazas
- ✓ Análisis avanzado de aprendizaje de comportamientos (usuario y apps)
- ✓ Arquitectura portátil de software
- ✓ Arquitectura distribuida
- ✓ Mercado Inmediato: Empresas Enfocadas a CU

Comunicación y Colaboración Segura

Para tratar con los crecientes problemas y retos de seguridad, RedShift Networks ha creado una línea de productos que ofrece:

1. “Proteccion” a través de un híbrido de identificación de amenazas estáticas aunado a un motor de aprendizaje adaptable y dinámico que identifica tráfico anormal en tiempo real.

2. “Visibilidad” por medio del análisis y reporte de sesiones y tráfico de redes de VoIP, CU y CEBP.

3. “Control” a través de un motor configurable de Aplicación de Políticas que permite que los administradores de IT aplacen, bloqueen o aceleren el tráfico que consideren indeseable.

RedShift Networks logra lo anterior sin sacrificar el desempeño ni la productividad de los empleados. RedShift Security Appliances ofrecen un punto de integración, visibilidad, control y protección para Comunicación Unificada Empresarial.

Acerca de RedShift Networks

RedShift Networks es líder en Comunicaciones Seguras y Soluciones de Colaboración. Somos los primeros en la industria en ofrecer soluciones de seguridad integrales para redes, sistemas y aplicaciones de Voz por IP, Video, Comunicaciones Unificadas 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.

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