REDSHIFT
NETWORKS
Secure Cloud Communication and Collaboration.

RedShift Networks UCTM vs. Nextgen Firewall

Overview

Redshift Networks is the leader in Unified Communications Threat Management (UCTM), the industry's first comprehensive security solution for IP Voice, Video, Unified Communications & Collaboration (UC&C) networks. The Core team is comprised of world-class executives from leading communication and system companies like Avaya, Cisco, SGI, Alcatel-Lucent, HP, Secure Computing and Ascend. RedShift's Board of Advisor's include some of the leading figures in the world of technology and academia. Founded in 2006, Redshift is headquartered in Silicon Valley with operations in India. Visit www.redshiftnetworks.com.

"Redshift Named Top 4 'Startups to Watch in 2009'" by Yankee Group – Leading Global IT Analyst

Unified Communication Market Today

Unified Communications & Collaboration Market is growing at a rapid pace with global companies such as Cisco, Microsoft, IBM, Avaya, Polycom, HP, Siemens, Alcatel and Google embracing the power of the new interconnected IP world to bridge traditional voice, data and video silo networks to bring powerful new UC/VOIP services never possible before. As a result, the traditional definition of security perimeter is now broken. With also the rise of new powerful fixed and mobile endpoint technologies such as the IPAD, the Android or IPhone smart phone, customers are now embracing UC/VOIP services at a potential never possible before. Hence, a strong need to protect these networks, applications and systems from an onslaught of attacks, threats and vulnerabilities is paramount. With the rise of complex networks, myriad endpoints and user behaviors, the need to have complete visibility and control of the UC network is also becoming very important to meet the growing compliance requirements.

Unified Comunications & Collaboration

« A New Era of Threats »

In 2008 attacks increased by 48%. We are all used to hearing about hackers, viruses, SPAM and other types of cyber attacks on data networks and the billions of dollars of losses they cause. Just as there are data threats, there are now a new set of threats and attacks that affect IP Voice, Video and UC&C networks.

WHY ENTERPRISES AND CARRIERS ARE DEPLOYING REDSHIFT UCTM

- Increased uptime and productivity due to better monitoring and elimination of UC/VOIP threats
- Compliance with security & regulatory rules requirements
- Prevent damage to Prestige and Image of the company
- Ensure business continuity
- Provide new, highly-valued security services to important customers with critical security concerns
- Become trusted unified communications security advisor to enterprise customers
- Single point of control for security and protection transversal functions for UC customers

RedShift Networks
UCTM vs. Nextgen Firewall

The Unified Communications & Collaboration realm is defined around real-time communications like: VOIP, Video Conferencing, Unified Messaging, Contact Center/Call Center applications, IVR & ACD systems, Presence, Collaboration, and a myriad of other communication applications. Some analysts have estimated that market will become a $35B market by 2013. Others have estimated an even faster growth pace as global enterprises have now aggressively begun to embrace these new technologies.

RedShift Secures Unified Communication & Collaboration networks, a $35B market by 2013.

UC&C security attacks in last 12 months

- *May 11'th, 2010 – FBI warns of IP Telephony Attacks*
- *April 14th 2010 - Amazon EC2 SIP Brute Force Attacks*
- *Dec 17th, 2009 – Predator Drones Hacked (Video Feeds)*
- *October 23rd, 2009 – Polycom VOIP Handsets Vulnerable*
- *October 20th, 2009 – Google Voice Mail Exposed – USA*
- *August 28th, 2009 – Skype Trojan Detected*
- *July, 6th, 2009 – Video ActiveX Flaw*

GARTNER (2007) — Enterprises that don't spend on IP Telephony Security today will end up spending 20% of their Security Operations Budget on it in 2011.

Unified Comunications & Collaboration

« Next Gen Firewalls Limitations »

» No complex UC&C Call state analysis & inspection
» No service application awareness
» No UC&C Zero Day defense
» No detailed UC & C Call reporting, incident management
» Suffer from similar high false positive rates similar to Data security solution (ie: IDS/IPS)
» No UC&C Behavioral analysis
» No real-time UC&C tracking and blocking for non compliant flow
» No UC&C infrastructure integration

Firewall with VoIP Capabilities

Traditional Data Firewalls such as Checkpoint UTM devices, NetScreen are beginning to add basic VOIP processing capabilities to their base UTM architecture. UTM firewalls are not best of breed devices as they tend to combine multiple security solutions with either no deep correlation of states between them, or defense-in-depth. The VOIP protocol processing in these solutions are usually limited to few syntactical checks for limited headers. The current data security architectures are not fundamentally well suited to handle real-time applications such as IP-Voice, Media, Unified Communication and Collaboration flows.

What Firewall with VOIP Capabilities can deliver:

» Securing data applications and protocols that are resilient to high degree of false-positives
» Policy-based visibility and control over applications, users and content
» A combination of application, user and data to uniquely identify an application, user or content type
» The depth of examination is usually limited to few packet header types
» Most of the core strengths lie around allowing or blocking certain types of applications or users
» Provides protection against viruses, Spywares, Worms and data threats/vulnerabilities using signatures
» Limited protection element available for few protocol anomaly tests and reactive signatures support.
» Basic URL filtering rules for sanitization of web traffic

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. Nextgen Firewall

What Firewall with VOIP capabilities cannot deliver:

- It does not maintain complex UC&C states (UC Stateful B2BUA). It is a requirement to effectively provide control, visibility & protection to UC&C network, applications and endpoints
- It does not actually handle or terminate the UC&C calls – a part function of a B2BUA. Hence, it's not aware of the deep call signaling, media and UC states.
- It can only understand the SIP, SCCP or H.323 packet as a packet from an application (i.e. Avaya Communication Manager, Cisco Call Manager, etc.)
- No 0-day defense-in-depth protection for 1000's of UC&C security threats and vulnerabilities (i.e. UC/VOIP Protocol fuzzing attacks, Toll Fraud, SPIT, media threats, Voice/UC DOS attacks, War Dialing, Presence Hijacking, data ⇨ voice threats etc.)
- No UC&C aware ACLs support or incident management
- The protocol anomaly checks are limited to few RFC implementations
- No tracking of UC services as it requires deeper cross-session correlations
- Data firewalls suffers from high false positives rates
- It cannot provide detailed UC call traffic analysis (i.e. detailed UC call processing, reporting, active states, call history, user anomalies etc)
- No media traffic statistics and reporting
- No detailed auditing and logging of all UC/VOIP session states, endpoints and user behaviors
- No integration with Unified Communication & Collaboration infrastructure (i.e. IP PBX, conferencing, Collaboration, Presence, Unified Messaging, call center, etc)
- Not able to track & block non-compliant UC traffic in real time

RedShift Networks UCTM Solution, Benefits and Advantages

- Easily deployable
- 100% QoS
- Five 9's Reliability
- Low latency overhead
- Near zero false positives
- Near zero false negatives
- High correlation of call and UC App states
- Full support of Real Time Communications
- Full support of complex heterogeneous network

Redshift Networks Solutions

Conventional Data security products such as Anti-SPAM, Virus, IDS/IPS, DB firewalls have grown to become multi-billion dollar markets within 4/5 years. Unified Communication and Collaboration is a new security problem.

RedShift Networks has created a unique High Performance Proactive Synchronous Flow Technology platform that provides comprehensive security solution for UC&C networks. The core detection technology is unique, protocol agnostic with several pro-active multithreaded detection engines that perform deep UC and VOIP call states handling, correlation and conformance detection. Four patents have been filed.

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. Nextgen Firewall

Unified Communications & Collaboration Security Requirements

UC&C Security Needs	Firewall	UCTM
UC/VOIP Protocol Anomaly Checks	Limited (voip)	Yes (voip/uc)
IP/TCP Infrastructure Threats	Yes	Yes
Voice/Video/UC DOS/DDOS Attacks – Flood, Stealth mode attacks	Limited (rated based, voice only)	Yes (rate/stealth/ voice/video/uc)
Spoofing prevention – Call-ID spoofing, Voice Phishing, Presence spoofing, identity theft	No	Yes
Voice/Video/UC Spam Attacks	No	Yes
Signaling Firewall – Toll Fraud, Fuzzing, Rate	No	Yes
UC/VOIP Vulnerabilities Lab & signatures	Partial	Yes (Condor)
UC Application Control	Partial	Yes
Call Routing Policies / Admission Control	No	Yes
Message Integrity Checks (SDP, HTTP, XMPP)	No	Yes
Media Firewall – Hijacking, Teardown, DOS	No	Yes
Signaling/Media Encryption (SIP/TLS, SRTP)	No	Yes
SIP Trunking security – DPI	Partial	Yes
Compliance / Privacy	Yes	Yes
Data Validation – Data ←→ Voice Threats	Yes	Yes
VOIP/UC aware AAA controls	No	Yes
UC Applications & Infrastructure Threats	No	Yes
UC Behavioral Analysis / Learning mode	No	Yes

Key Difference

- UCTM maintain complex call states processing for UC stateful B2BUA; required to effectively provide control, visibility & protection to UC&C network, applications and endpoints
- Redshift UCTM is managing 0-Day threats
- Redshift UCTM operates at UC/ VOIP Services level
- Redshift UCTM full UC&C detailed reports (E.g. detailed UC call processing, Active states, call history, User Anomalies)
- Redshift UCTM is fully integrated with communication infrastructure elements

In Summary

NextGen Firewall performs well for traditional IT Data security solutions. However, it is not clearly suited to protect real-time UC&C networks.

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