使用 UserLock 限制 Wi-Fi 和 VPN 会话 保障 Windows 网络的自带设备安全

www.isdecisions.com



使用 UserLock 限制 Wi-Fi 和 VPN 会话 保障 Windows 网络的自带设备安全

自带设备(即 BYOD,全称为 Bring Your Own Device)安全一直是很多 IT 部门关注的问题。知名网络安全监控软件 UserLock 最新版本(UserLock7)新增了对 Wi-Fi和 VPN 会话的监控功能,允许公司对他们的无线网络进行监控,确保有安全的 BYOD 环境。

使用 UserLock, 公司可以对所有 Wi-Fi 和 VPN 会话进行监控、限制和记录。

如何使用 UserLock7 限制 Wi-Fi 和 VPN 会话

下面的简图显示了 UserLock 管理 RADIUS (RADIUS,即远程认证拨号用户服务,是一种 认证协议。)认证的 VPN 和 Wi-Fi 会话的原理:

Windows 认证的 VPN



RADIUS 认证的 VPN







RADIUS 认证的 Wi-Fi



RADIUS 认证的 Wi-Fi 和 VPN







通过限制 Wi-Fi和 VPN 会话,你能对网络访问进行更有效的监控。

为你的网络安装 UserLock 代理

要求:

- 对于 VPN 会话:经 RADIUS 服务器认证的 RRAS 服务器 (RRAS,即路由与远程访问服务,是微软管理 VPN 会话的一 种技术,RRAS 服务器可以与 Windows 认证或 RADIUS 认证进 行配置。)或 VPN 服务器
- 对于 Wi-Fi 会话:访问点与 RADIUS 兼容

安装:

对于 VPN 会话:

• 在 RRAS 服务器上安装 RRAS UserLock 代理

4



• 或在认证 VPN 服务器的 RADIUS 服务器上安装 IAS (RADIUS) UserLock 代理

对于 Wi-Fi 会话:

• 在认证 Wi-Fi 访问点的 RADIUS 服务器上安装 IAS (RADIUS) UserLock 代理

为受 UserLock 保护的帐户配置 Wi-Fi 和 VPN 限制。

使用:

在下面的案例中,你可以看到如何为受保护的账户进行配置,使对于所有用户都只允许一个 Wi-Fi和 VPN 会话。

1.为 VPN 服务器配置 RADIUS 认证指定的 IAS (RADIUS) 服务器(名称和密码)。

Kouking and	Describe Armede						
Server S	emote Access V5523201RAS (local)						
VSS2320	RAS (local) Welcome to Pouting and Remote Access						
	S523201RA5 (local) Properties	? X mote access to private	networks.				
Por	General Security IP PPP Logging	RADIUS Authentication	?				
0- <u>3</u> pr	The authentication provider validates credentials for remote access clier	The following BADIUS servers an	e queried in order from the binhest to the				
	and demand-dial routers.	lowest score.	e queneu in order nom the nightest to the				
	Authentication provider:	Server	Initial Score				
	RADIUS Authentication Configure	Discourse of the	200				
	·	V5526402HA5	30				
	Authentination Methods	V55264U2HA5	30				
	Authentication Methods	V5526402HAS	30				
	Authentication Methods	VS526402HAS	30				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions.	V5526402HAS	30				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions. Accounting provider: RADULS Accounting	V5526402HAS	30				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions. Accounting provider: RADIUS Accounting Configure	V5526402HAS	30				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions. Accounting provider: RADIUS Accounting Configure The custom IPSec policy specifies a pre-shared key for L2TP connection The Routing and Remote Access service should be started to set this option.	VS526402HAS	30				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions. Accounting provider: RADIUS Accounting Configure The custom IPSec policy specifies a pre-shared key for L2TP connection The Routing and Remote Access service should be started to set this option. Allow custom IPSec policy for L2TP connection	Add	su				
	Authentication Methods The accounting provider maintains a log of connection requests and sessions. Accounting provider: RADIUS Accounting	<u>Ad</u>	30 4] <u>E</u> dit] <u>R</u> emove				

2.将 Wi-Fi访问点设置为 RADIUS 认证指定的 IAS 服务器。



Wireless Settings					
Wireless Band	IEEE802.11g +				
Mode	Access Point -				
Wireless Network Name(SSID)	CORP				
SSID Broadcast	Enable -				
Channel	13 - 2.472 GHz Auto Channel Scan				
Authentication	WPA-EAP -				
RADIUS Server Settings					
C.L. T.	AUTO - Group Key Update Interval				
Cipher Type	1800				
Primary radius server setting	ng				
RADIUS Server	192.168.1.1				
RADIUS Port	1812				
RADIUS Secret	•••••				
Secondary radius server se	etting				
Secondary RADIUS Mode	Disable -				
RADIUS Server					
RADIUS Port	1812				
RADIUS Secret					
Primary accounting server	setting				
Accounting Mode	Enable -				
Accounting Server	192.168.1.1				
Accounting Port	1813				

3.在 IAS 服务器上安装 IAS UserLock 代理。







4.将受保护的账号设为"Everyone",使所有用户与新规则关联。勾选"允许 Wi-Fi 和 VPN 会话"并在后面的框中填写数字"1"。

	Configuration Properties for Everyone ×				
Welcome Servers	General				
▼ SERVER1	Account name Everyone				
Protected accounts	Number of concurrent sessions allowed	Custom session limits			
Messages User sessions Agent distribution	Allowed workstation sessions Allowed terminal sessions Total allowed interactive sessions Allowed Wi-Fi / VPN sessions Allowed IIS sessions Allowed IIS sessions	Limit Session type			

5.将某个账户与 VPN 连接,连接成功后,你能在 UserLock 控制台看到会话。

• UserLock	Servers • SER\	/ER1•User se	essions					
	Configuration							
w Welcome w Servers w SERVER1	USER SESSION	S SERVER1						
Protected accounts Messages				-	Find	Clear		
User sessions	User name	User account	Sessions		Session		Session status	Session t
Agent distribution	Myadmin	Myadmin	1	. 2	10.239.0.10/G	1	Open	Wi-Fi &

6.试与该账户进行 Wi-Fi 连接,连接被拒绝。

7.关闭该账户与 VPN 的连接,再与 Wi-Fi 连接,连接被允许。

在 Wi-Fi 和 VPN 会话中,使用 UserLock 还可以对以下两方面进行限制:

- 定义工作时长
- 时间配额

