IP/MAC/Hostname-Based Network Access Controls

Technical Note

ViASC@pe usa

IPScan can be used to register specific, required MAC address, IP address and Hostname combinations for gaining network access, and to enable blocking of violating MAC/IP/Hostname combinations as well as unknown MAC and IP addresses. Specifically, IPScan can defined policies that require:

- That only a single or multiple defined IP addresses may be used with a specific MAC address
- That only a single or multiple defined MAC addresses may be used with a specific IP address
- That only a single defined hostname may be used with a specific MAC address

Definition of these policies can be done after automatically scanning all the active IP devices on the network, so that all the administrator needs to do is confirm the current settings being used on the network. This auto-detection and policy registration capabilities greatly decreases the manual labor needed to register and define per user network access control policies.

Policy definition can be performed on a per probe or on a network-wide basis by opening a view of IP devices on the network in the IPScan Console (these can be viewed inclusively or based on whether they are online or offline), right clicking on one more IP devices, then selecting the Apply MAC/IP registration options, as seen in figure 1:

Ę	No	IP Address		MAC Address		dress	Apply		Host Nam	Host Name		Name	NIC Vendor	1	
Real-time	1	SMU 192.1	SMU 192.168.100.			1 00-E0-4C-77-CE-CC				Unknown	Unknown		own	REALTEK SET	110
å	2	8881 192.1	58.	DOS Commands			•		IPSCANPE	IPSCANPROBE 5		E	Scope Inform	Scope Informat	
	3	8881 192.1	58.	Copy Data Check IP Status					Unknown		Unkno	own	Scope Inform	at	
20	4	SIII 192.1	58.						Unknown		Unkno	own	Scope Inform	at	
Policy 🔆	5	8881 192.1	58.	Check IP Status				_		Unknown Unk		Unkno	own	Scope Inform	Scope Informat
ije	6	88.192.1	58.	IP Return Delete MAC Delete Row Apply IP/MAC Blocking Remove Blocking					Unknown		Unkno	own	Scope Inform	at	
a	7	SIII 192.1	58.						MINDORY			E-RND	Unknown		
	8	SEII 192.1	58.						DHOH-S0			KGROUP	ASUSTEK CO	MF	
	9	SIII 192.1	58.				_		Unknown		Unkno	own	REALTEK SEI	AIC	
	10	SIII 192.1	58.						NAME2		WOR	KGROUP	3COM CORP	JF	
	11	SIII 192.1	58.				•		BLUESKY4	9	WORKGROUP		3COM C RP	JF	
Events	12	SMU 211.2	32.	Apple	MACITE	Registration			_				חיך	REALTEK SET	110
	13	SS 211.2	32.	_			_	-8	_	ly IP Reg. Bloc	N		ROUP	IBM CORPOR	A
	14	SSI 211.2	32.	Remo	emove MAC/IP Registration			R	Apply IP Reg. Log Only 🗟 ROUP			ROUP	3COM CORPOR		
_	•			Syste	System Device Group				Apply MAC Reg. Blocking						•
_				Remo	ove from :	System Device	e Group	Q		ly MAC Reg. L	og Only				
				Broa	dcast limit	free device			App	ly Hos <u>t Nam</u> e R	eg. Blo	cking			
				Time	ime Control 🙀 Apply og Only										
				Remo	ove Time	Control		•		\sim					
				Save	as CSV F	ile		•			8)	\ \		
				IDEc	an Cons	ala						2			
				IF SC	ancons	FUIE						1			
				6	ГТС	Rea Block	kinal D			nt to execu	to the	comm	and2		
				0		- Keg, bloc	king] t	/O yc	u wa	In to execu	te trie	comm			
					4-										
						ſ	Yes		1	No					

Figure 1: Implementing MAC/IP/Host based network access controls with IPScan

Viasc@pe usa

After implementing MAC/IP/Hostname policy restrictions on network access, the network administrator can apply new IP and MAC address blocking to prevent unknown addresses from accessing the network. This option is implemented at the probe level in the IPScan Console and is performed separately for new IP blocking and new MAC blocking, as shown in Figure 2:

记 Probe	1	Group
viascop	1	Check Probe Connection ARP Probe Segment
		Safety Mode
		New IP Blocking
		Manage Available IP
		New MAC Blocking (Probe)
		New MAC Bloc IPScan Console
		Add MAC
		Off Range Bloc [192.168.100.20] New IP Blocking Do you want to execute the command?
		Expired IP/MA
		Broadcast Allo
<u> </u>		Broadcast Violation Blocking
		Add Group
		Create C Class Groups
		Delete Probe Gra
		Delete Probe New IP Blocking: Successfully defined!
		View Data
		Monitoring Rang OK
		Telenet Access terrose
		Probe Change

Figure 2: New/Unknown IP and MAC address blocking enabled in IPScan

By applying MAC/IP/Hostname policies to known IP devices, then implementing automatic blocking of new and unknown MAC and IP addresses, network managers can ensure the integrity of basic IP network access control across all IP devices, whether their IP addresses are statically or dynamically assigned.

IPScan is the only solution that provides full management, access control and auditability of all IP devices on the network. Deployed in production by dozens of global Fortune 2000 enterprises, government and military organizations, Services Providers and educational institutions, IPScan is the leading IP/MAC access control solution.

Viasc@pe usa