## Activation SNMP sur un pare-feu WatchGuard

## Via l'interface WEB

Une fois connecté, vous arrivez sur le tableau de bord du pare-feu comme sur l'image ci-dessous.

WatchGuard	Fireware Web UI								
TABLEAU DE BORD Panneau avant Services d'abonnement	Panneau avant Principaux clients Tout afficher Principales destinations								
FireWatch	NOM	DÉBIT 🖨		OCTETS		VISITES	NOM	DÉBIT 🖨	
Interfaces		_	192 мbps		4,364 мв	53	10.0.0.8		267 м
Traffic Monitor		_	76 Mbps	(	1,664 мв	81		-	35 мыр
Controleur sans fil de passerelle Geolocation			14 Mbps	C	1,272 мв	41	10.0.0.21	•	18 мыр
Sécurité mobile			14 Mbps	(	702 мв	52	172.21.0.195		14 мвр
Découverte de réseau			9 Mbps		216 мв	2	10.0.0.42	(	8 Mbps
ETAT DU SYSTEME		•	9 Mbps		115,017 мв	33	10.0.0.9		3 Mbps
RESEAU			8 Mbps		4,110 мв	57	192.168.81.52		2 Mbps
			8 Mbps		1,413,487 мв	1	10.0.3.10		1 Mbps
			6 Mbps		113 мв	9			895 кы
RÉSEAU PRIVÉ VPN (VIRTUAL		-	3 Mbps		5 мв	5	_		632 кр
PRIVATE NETWORK)	Principales applicat	ions				Tout officher	Principales stratéo	ios	
SYSTÈME		10113				Tout anicher	Fincipates strateg		
	NOM	DEBIT Ç		OCTETS	45	VISITES	NOM	DEBIT 🤤	267
	Youtube	C	1 Mbps	-	15 мв	10			267 MI
	Amazon CloudFront	(	227 Корз	(	5 мв	9		•	31 мыр
	HTTP Protocol over TLS SSL	C	64 Kbps		21 мв	93	Camera1-int	•	18 мыр
	Microsoft.com	C.	22 Kbps	(	Змв	29		•	15 мыр
	Microsoft Teams	÷	14 Kbps	<u> </u>	Змв	22		(	8 Mbps
	Microsoft Windows Update	C	8 Kbps		56 кв	9			3 Mbps

Cliquez sur « System » et ensuite sur « SNMP », vous arriverez sur la page de configuration SNMP. Comme ci-dessous :

WatchGuard	Fireware Web UI				
TABLEAU DE BORD	SNMP				
ÉTAT DU SYSTÈME	Chi uez sur le verrou pour effectuer des changements				
RÉSEAU					
PARE-FEU	Paramètres SNMP				
SERVICES D'ABONNEMENT	Version	v1/v2c V			
AUTHENTIFICATION	Chaīne de communauté	public			
RÉSEAU PRIVÉ VPN (VIRTUAL					
PRIVATE NETWORK)	Nom d'utilisateur				
SYSTÈME	Protocole d'authentification	MDE V			
		mus T			
	Mot de passe				
SNMP	Carrieran (C)				
	commer(c)				
	Protocole de confidentialité	DES			
	Mot de passe				
	Confirmer (C)				
	INTERROPTIONS SIN	vie Vie			
	version				
	v1Trap	×			
	Station de destion SN				
	ADRESSE IP (1)				
Apropos	Utiliser la NAT pour les conn	exions dar ALG (Addication Laver Gateway) SNMP			

Cliquez sur « Cadenas » en haut à gauche pour déverrouiller la page de configuration et ensuite saisissez les informations dont vous avez besoin (communité, version SNMP (si v3 l'authentification)

Si vous utiliser les TRAP, vous devez également renseigner les adresses des serveurs autorisés. Suite à la validation de cette fonction, une règle NAT va se créer :

WatchGuard	Fireware Web UI					
TABLEAU DE BORD ÉTAT DU SYSTÈME RÉSEAU PARE-FEU Strategies de pare-feu	Strategies de pare-feu / Modifier (E)       Image: Cliquez sur le verrou pour effectuer des changements       Nom     SNIMP-Lan-Firebox					
Strategies IPSec Mobile VPN Alias Actions de proxy Actions de Contenu Profils TLS Gestion du Trafic	Parametres     SD-WAN     Application Control     Geolocation     Gestion du Trafic     Plantification     Avances       Les connexions sont     Autorisé     ✓     ✓					
Planification SNAT Gestion des paquets par defaut Sites bloques Ports bloques Quotas SERVICES D'ABONNEMENT	DE ♠ À ♠					
AUTHENTIFICATION RÉSEAU PRIVÉ VPN (VIRTUAL PRIVATE NETWORK) SYSTÈME	Activer Intrusion Prevention Service Activer des quotas de bande passante et de durée Bloquer automatiquement les sites qui tentent de se connecter Definir un delai d'inactivite personnalise 180 Secondes					
	Journalisation  Triver un message de journal  Frivoyer un message du journal pour les rapports  Frivoyer une interruption SNMP  Frivoyer une notification  Friver contextuelle Intervalle de lancement ISTREE					

Dans le champ DE : rentrer les adresses IP du ou des serveur(s) de supervision

Enregistrez la configuration.

SNMP est maintenant activé sur votre pare-feu WatchGuard.

## Via l'interface du client lourd

Une fois que vous avez ouvert le Policy Manager, cliquez sur Setup et SNMP

Configurez ensuite le composant avec vos informations :

SNMP Settings						
SNMP Polling	1					
User Name:						
Authentication Protocol: MD5 V Password:						
Con firm:						
Privacy Protocol: DES V Password:						
Con firm:						
SNMP Traps: v1Trap v						
SNMP Management Stations	7					
Add Remove						
✓ Use NAT for connections through the SNMP application layer gateway (Fireware OS v11.9.4 and higher)						
OK Cancel Help						

Une fois validé, modifiez la règle SNMP créer par le firewall en spécifiant les adresses du ou des serveur(s) de supervision

R		Edit Policy Properties	×			
Name: SNMP-L	an-Firebox		🖌 Enable			
Policy Propert	ies Advanced					
SNMP connection	ons are					
Allowed	¥	Send TCP RST				
		Add Edit F	Remove			
To						
		Add Edit F	Remove			
Route out	bound traffic using	SD-WAN Based Routing V (Fireware OS v12.3 or higher)	)			
SD-WAN A	ction					
Enable App	lication Control:	Global 🗸 📝 🖿				
Enable Geo	location	Global 🗸 📝 💽				
Enable IPS	✓ Enable IPS for this policy					
Enable ban	Enable bandwidth and time quotas (Fireware OS v11.10 and higher)					
Proxy action:						
		OK Cancel	Help			

Cliquez sur OK.

SNMP est maintenant activé

