

IPS/IDS Firewall Setup

By clicking on the **Threat Scanning** tab located in the top panel of the **Firewall** page you can set the initial alerting and blocking rules for the particular customer as seen in Figure 1. This is done on a per client basis however the alerts for each site may vary greatly. It is here where you can also set email alerting for this particular customer.

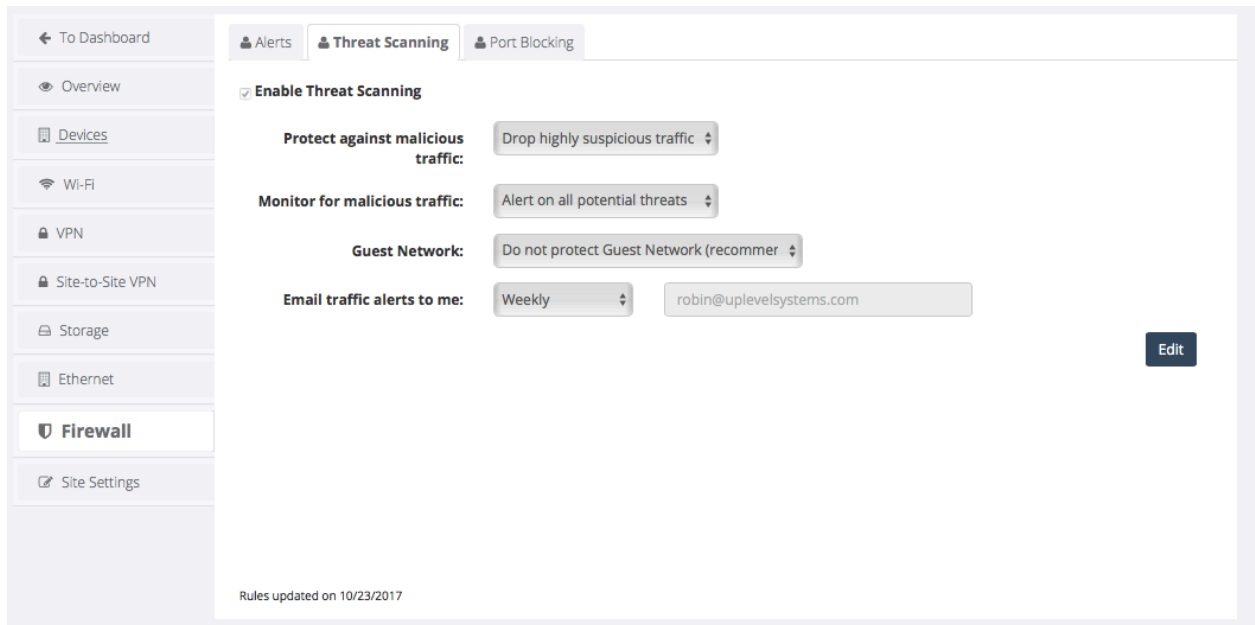



Figure 1 – Threat Scanning Rules

Once these rules are initially set you will begin to see alerting on the traffic in the **Alerts** tab located at the top of the **Firewall** tab as seen in Figure C.

Alerts		Threat Scanning	Port Blocking	Exceptions	
Type	Description	Addresses	Time		
Alert: successful-recon-limited Rule 1:29456	PROTOCOL-ICMP Unusual PING detected	ICMP, Local: USAU-300925-L, Internet: 13.65.245.138	10/18 08:00am	⋮	
Alert: shellcode-detect Rule 1:1394	INDICATOR-SHELLCODE x86 inc ecx NOOP	TCP, Local: Robins-MBP, Internet: 173.194.24.168	10/18 02:26am	⋮	
Alert: misc-activity Rule 1:408	PROTOCOL-ICMP Echo Reply	ICMP, Local: USAU-300925-L, Internet: 52-114-188-18.relay.teams.microsoft.com	10/17 09:56am	⋮	
Alert: successful-recon-limited Rule 1:29456	PROTOCOL-ICMP Unusual PING detected	ICMP, Local: USAU-300925-L, Internet: 52-114-188-18.relay.teams.microsoft.com	10/17 09:56am	⋮	
Alert: system-call-detect Rule 1:650	INDICATOR-SHELLCODE x86 setuid 0	UDP, Local: USAU-300925-L, Internet: 64.157.241.251	10/17 09:11am	⋮	
Alert: bad-unknown Rule 1:254	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	UDP, Local: USAU-300925-L, Internet: ip-192-168-1-254.us-west-2.compute.internal	10/15 10:57pm	⋮	
Alert: system-call-detect Rule 1:650	INDICATOR-SHELLCODE x86 setuid 0	TCP, Local: Robins-iPhone-2, Internet: a23-206-195-64.deploy.static.akamaitechnologies.com	10/14 06:11pm	⋮	

Figure C – Alerting

It is here that you can begin to create rules for each individual alert profile. The IPS/IDS firewall uses linux based Snort to characterize profiles. These rule profiles can be seen in each alert, ex: [Rule 1:29456](#) these rules can be Googled to get a more in depth explanation about the exact threat profile. Applications can not work by blocking everything so it is important to understand what it is exactly that is flowing through the network and what of that should be blocked. Once a threat has been identified you can press the  symbol to the right of each alert to identify how the profile should be handled moving forward as seen in Figure D.

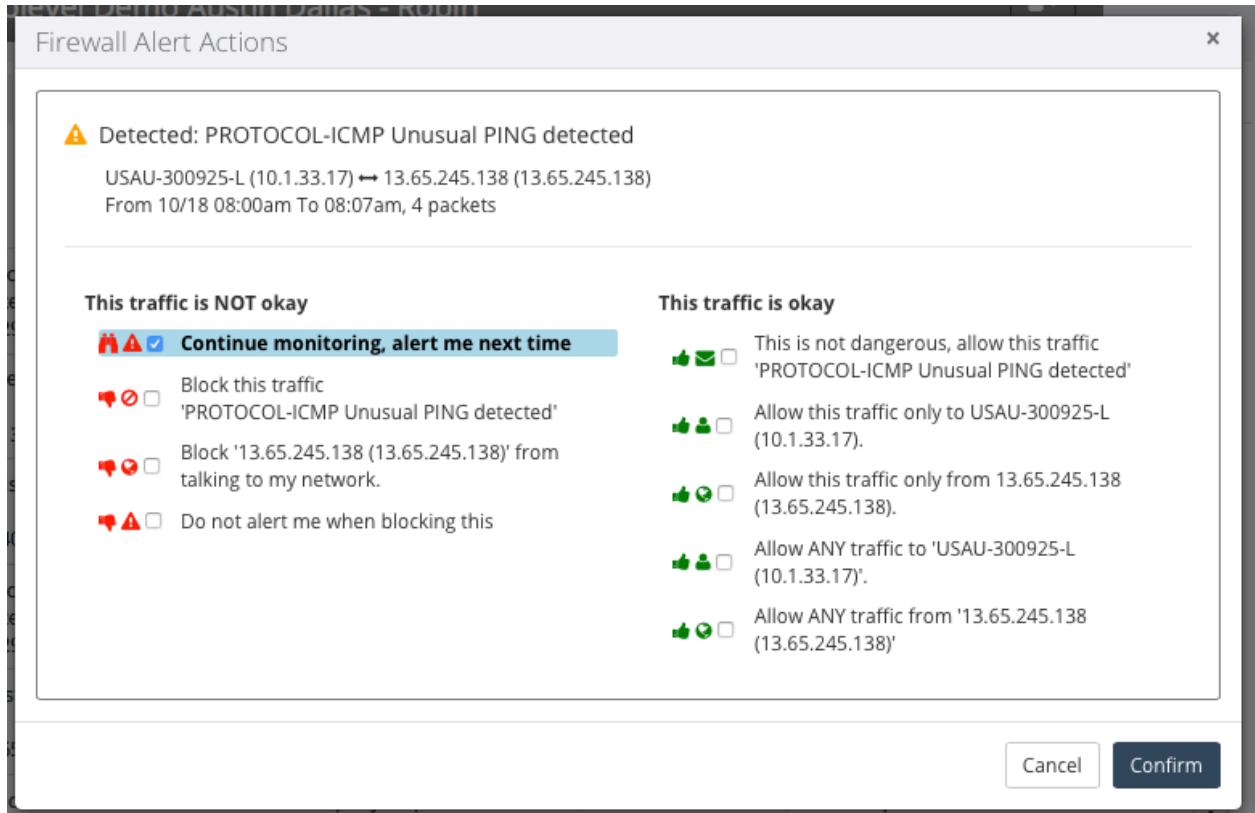


Figure D – Firewall Alert Actions

This allows for you to specific pick how to handle the traffic in the future with a similar attack profile. Once the rule has been confirmed you can click Exceptions in the top right hand corner of the alerting page to view all previous profile rules allowing you to delete them in the future (Figure E).

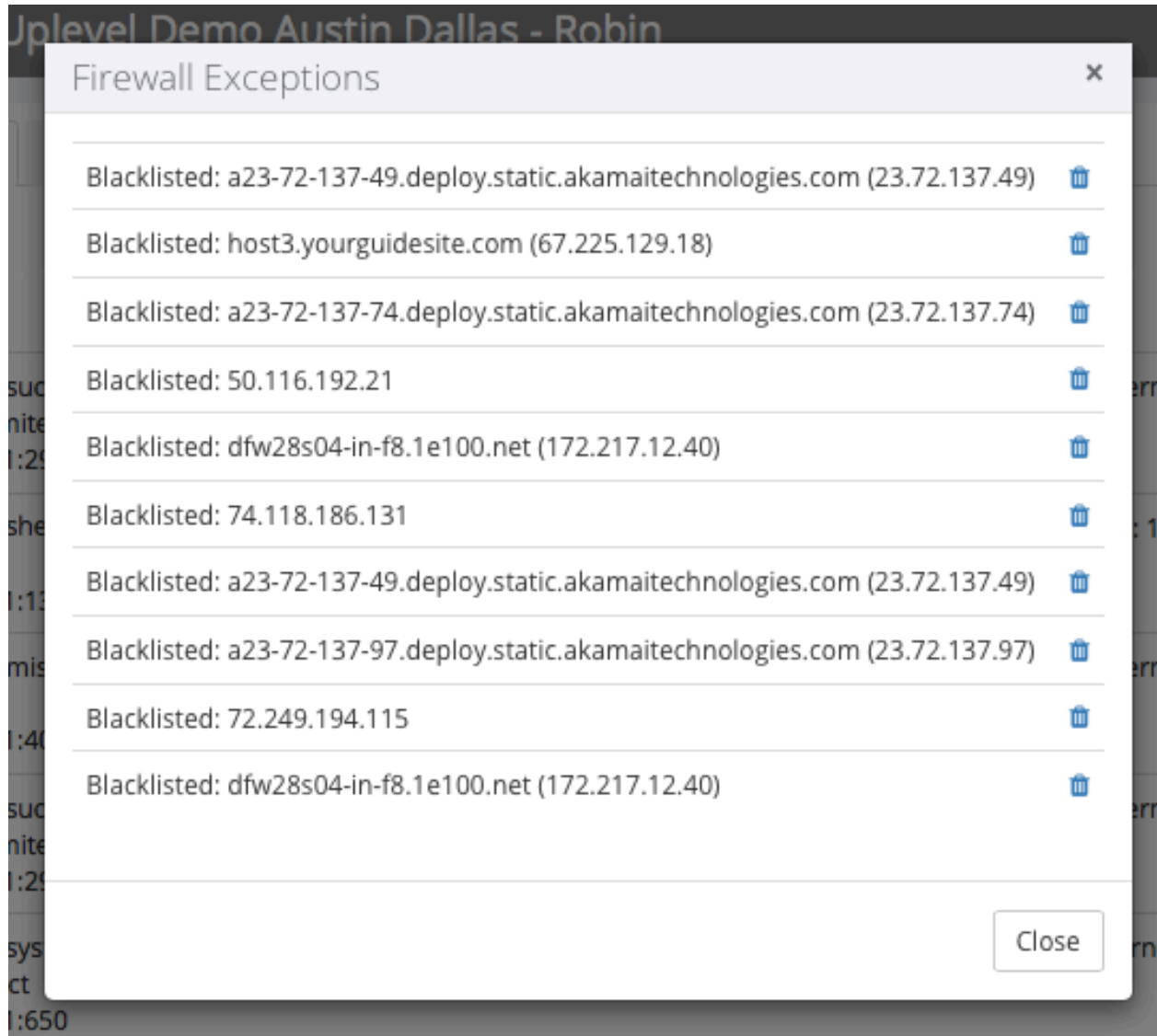


Figure E – Firewall Exceptions

Please note that by enabling the IPS/IDS firewall it is then subject to the throughput power of the processor of 30Mbps. For business with a larger bandwidth they may experience a lowering of their speeds when using the IPS/IDS Firewall. This is to be expected and a typical value on the market. This value varies based on the quantity and type of traffic flowing through the firewall.