



# SONICWALL FIREWALL BEST PRACTICES



March 2017

Bobby Cornwell  
Sr. Manager, Sales Engineering

# FIRST STEP OUT OF THE BOX

- Start from Safemode: (Recommended)

- Enter Safemode by booting up the firewall – then using a paper clip or similar sized item, insert into the small hole either in front or back of the firewall, and hold the “button” down for 10 seconds or more. The wrench light will start flashing, and you can release the “button”
- Load latest firmware and boot to factory defaults\*
  - Safemode is not required but is the most cautious method and leaves least room for technology induced issues

- If you do not start from Safemode, do the following:

- Skip Setup Guide (Wizard)
- Register the appliance (you cannot load firmware unless the appliance is registered (if you are not in Safemode))
- Load latest firmware and boot to factory defaults\* \*Reason: Issues in configuration created in old/initial release RTM firmware can survive firmware upgrades; this step eliminates this chance, however small it may be.

# SETTINGS TIPS

Mode: Configuration ▶

Accept Cancel

### Settings

Import Settings... **Export Settings...** Send Diagnostic Reports to Support

### Firmware Management

**Note:** Backup Settings were created THU OCT 20 10:03:18 2016 from version SonicOS Enhanced 6.2.6.1-24n

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 6.2.6.1-24n	THU OCT 20 03:45:39 2016	72.00 MiB	↓	⏻
Current Firmware with Factory Default Settings	SonicOS Enhanced 6.2.6.1-24n	THU OCT 20 03:45:39 2016	72.00 MiB	↓	⏻
System Backup	SonicOS Enhanced 6.2.6.1-24n	THU OCT 20 03:45:39 2016	72.00 MiB	↓	⏻

Upload New Firmware... **Create Backup...**

Boot with firmware diagnostics enabled (if available)

### Firmware Auto-Update

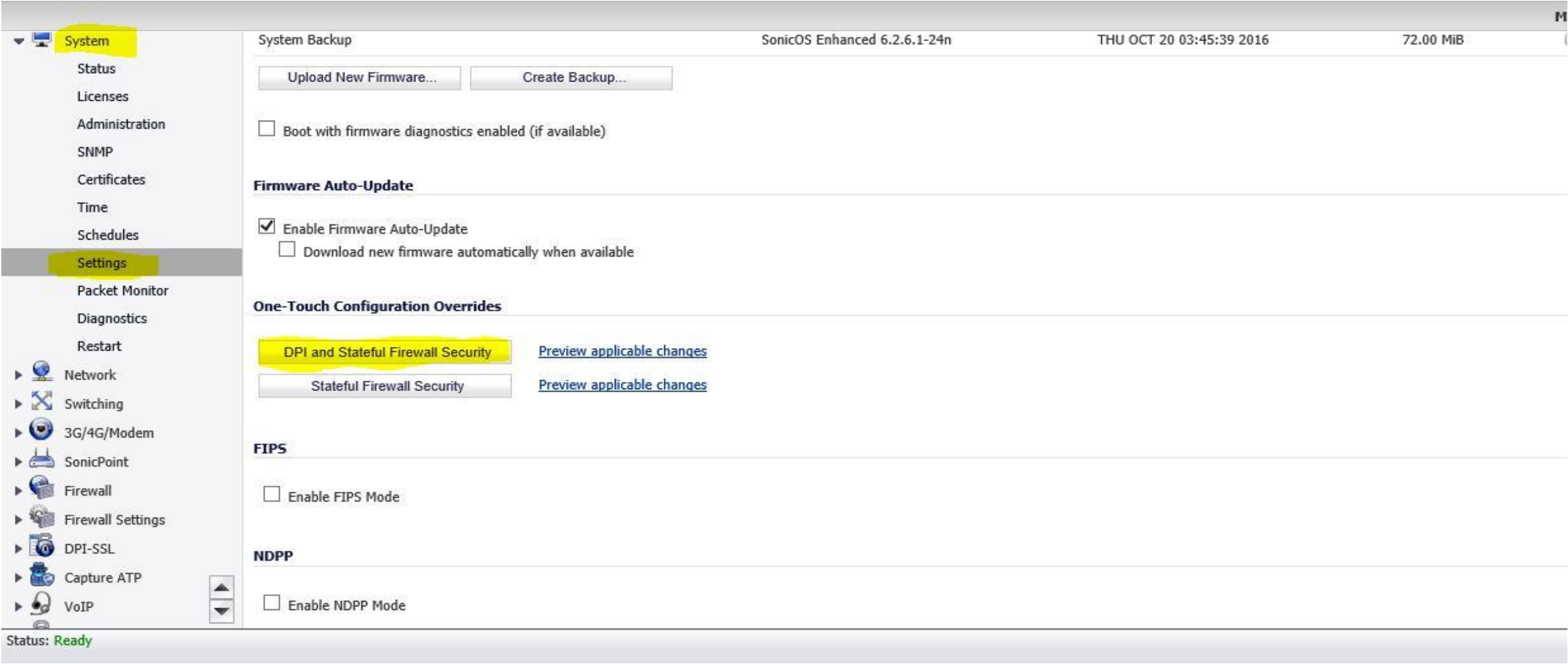
## “BENCH” CONFIGURATION (IF YOU ARE NOT CONNECTED TO THE INTERNET)

- Licenses: System >>> Licenses
  - View then copy firewall’s license keyset from firewall’s MySonicWALL page and paste into System >>> Licenses page
- Signature Database: System >>> Security Services
  - Download latest countermeasure database (‘signature file’) from firewall’s MySonicWALL page and upload via Security Services >>> Summary >>> Import Signatures

# SYSTEM

- System >>> Administration
  - For PCI/Better Security: Change super user administration account from 'admin'
  - Enable Enhanced Audit Logging (new in 6.2.5 for UC APL certification)
  - Change HTTPS management port from 443 to other (i.e. 8443)
  - Change the default Admin Timeout from 5 minutes, to your preferred amount
- System >>> Time
  - Set time automatically using NTP
  - Don't configure additional NTP Servers unless needed for internal synchronization
- System >>> Diagnostics
  - Check Network Settings
    - Note that "Content Filtering" will fail until licensed or if UDP/2257 is blocked from SonicWALL Firewall to SonicWALL GRID CFS Servers. <https://support.software.dell.com/kb/sw9405>
  - MTU Discovery: Paste determined value into WAN/Internet interface used in test
    - Note: Some ISP's values change each time you test. In that case review ISP's KB for optimum MTU

# ONE TOUCH SECURITY CONFIGURATION



The screenshot shows the SonicWall One Touch Security Configuration interface. The left sidebar contains a navigation menu with categories: System, Settings, Network, Switching, 3G/4G/Modem, SonicPoint, Firewall, Firewall Settings, DPI-SSL, Capture ATP, and VoIP. The main content area is titled "System Backup" and includes the following sections:

- System Backup:** Contains buttons for "Upload New Firmware..." and "Create Backup...". A checkbox for "Boot with firmware diagnostics enabled (if available)" is present and unchecked.
- Firmware Auto-Update:** Contains a checked checkbox for "Enable Firmware Auto-Update" and an unchecked checkbox for "Download new firmware automatically when available".
- One-Touch Configuration Overrides:** Contains a highlighted button for "DPI and Stateful Firewall Security" with a link for "Preview applicable changes". Below it is a button for "Stateful Firewall Security" with another link for "Preview applicable changes".
- FIPS:** Contains an unchecked checkbox for "Enable FIPS Mode".
- NDPP:** Contains an unchecked checkbox for "Enable NDPP Mode".

At the top right of the interface, the following information is displayed: "SonicOS Enhanced 6.2.6.1-24n", "THU OCT 20 03:45:39 2016", and "72.00 MiB". At the bottom left, the status is "Ready".

# ONE TOUCH CONFIGURATION

Using the One-Touch DPI and Stateful Firewall high security applies the following configurations to the system. A system restart is then required for the updates to take full effect.

## *System>Administration*

1. Password must be changed every 90 days
2. Bar repeated password changes for 4 changes
3. Enforce password complexity: Require alphabetic, numeric and symbolic characters
4. Apply the above password constraints for: all user categories
5. Enable administrator/user lockout
6. Failed Login attempts per minute before lockout: 7
7. Enable inter-administrator messaging
8. Inter-administrator Messaging polling interval (seconds): 10

## *Network>Interfaces*

9. Any interface allowing HTTP management is replaced with HTTPS Management
10. Any setting to 'Add rule to enable redirect from HTTP to HTTPS' is disabled
11. Ping Management is disabled on all interfaces

## *Network>Zones*

12. Intrusion Prevention is enabled on all applicable default Zones
13. Gateway Anti-Virus protection is enabled on all applicable default Zones
14. Anti-Spyware protection is enabled on all applicable default Zones

## *Network>DNS*

15. Enable DNS Rebinding protection
16. DNS Rebinding Action: Log Attack & Drop DNS Reply

## *Firewall>Access Rules*

17. Any Firewall policy with an Action of Deny, the Action is changed Discard
18. Source IP Address connection limiting with a threshold of 128 connections is enabled for all firewall policies

# ONE TOUCH CONFIGURATION

## *Firewall Settings>Advanced*

19. Turn on Enable Stealth Mode
20. Turn on Randomize IP ID
21. Turn off Decrement IP TTL for forwarded traffic
22. Connections are set to: Maximum DPI Connections (DPI services enabled)

## *Firewall Settings>Flood Protection*

23. Turn on Enable TCP handshake timeout

## *VPN>Advanced*

24. Turn on Enable IKE Dead Peer Detection
25. Turn on Enable Dead Peer Detection for Idle VPN sessions
26. Turn on Enable Fragmented Packet Handling
27. Turn on Ignore DF (Dont Fragment) Bit
28. Turn on Enable NAT Traversal
29. Turn on Clean up Active tunnels when Peer Gateway DNS name resolves to a different address
30. Turn on Preserve IKE port for Pass Through Connections

## *Security Services>Gateway Anti-Virus*

31. If licensed, Enable Gateway Antivirus
32. Configure Gateway AV Settings: Turn on Disable SMTP Responses
33. Configure Gateway AV Settings: Turn off Disable detection of EICAR test virus
34. Configure Gateway AV Settings: Turn on Enable HTTP Byte-Range requests with Gateway AV
35. Configure Gateway AV Settings: Turn on Enable FTP REST request with Gateway AV
36. Configure Gateway AV Settings: Turn off Enable HTTP Clientless Notification Alerts

## *Security Services>Intrusion Prevention*

37. If licensed, Enable IPS
38. Turn on Prevent All and Detect All for High Priority Attacks
39. Turn on Prevent All and Detect All for Medium Priority Attacks
40. Turn on Prevent All and Detect All for Low Priority Attacks



# ONE TOUCH CONFIGURATION

## *Security Services>Anti-Spyware*

41. If licensed, Enable Anti-Spyware
42. Turn on Prevent All and Detect All for High Priority Attacks
43. Turn on Prevent All and Detect All for Medium Priority Attacks
44. Turn on Prevent All and Detect All for Low Priority Attacks
45. Configure Anti-Spyware Settings: Turn on Disable SMTP Responses
46. Configure Anti-Spyware Settings: Turn off Enable HTTP Clientless Notification Alerts

## *Log>Settings*

47. Set Logging Level: Debug
48. Set Alert Level: Warning

## *Log>Name Resolution*

49. Set Name Resolution Method to: DNS then NetBIOS

## *Internal Settings*

50. Turn on Protect against TCP State Manipulation DoS
51. Turn on Apply IPS Signatures Bidirectionally
52. Allow launching of AppFlow monitor in stand-alone browser frame
53. Enable Visualization UI for Non-Admin/Config users


# NETWORK

- Network >>> Interfaces
  - Link Speed: Set to Auto or, if possible, hard code on both sides to best possible (i.e. 100/full duplex, 1 Gb)
  - WAN Interfaces and enabling management (don't open to whole world):
    - Create Address Objects for external IP addresses that can manage device
    - Add those to new Address Object Group created for this purpose
    - Edit WAN:WAN HTTPS and HTTP Management auto rules and change Source to newly created group  
(Note: Alternatively VPN first to manage firewall)
- Network >>> Zones
  - Make sure all desired security services are enforced on proper zones
- Network >>> Services:
  - “Any” in firewall policy does not mean ‘any’ unless firewall knows about the service. Therefore, add any Services required but not present.
  - Log Event ID 41: Network Access >>> Unknown Protocol Dropped will expose these

# NETWORK ADDRESS TRANSLATION

- On outbound policy, select specific outbound Interface (Not recommended to use “Any”)
- On inbound policy, select specific inbound Interface (Public Server Wizard sets this to Any)
- If you use Public Server Wizard:
  - Only use once to show/use as a reference then manually create additional Firewall/NAT policies
    - While the Wizard is good for creating a quick policy, it’s recommended to build policies manually for learning purposes (not to mention the Wizard creates 3 policies each time).
  - Rename & change PSW inbound NAT policy’s inbound Interface from Any to specific interface
- Don’t create unnecessary Loopback policies
- Outbound Many-to-Few : Use Address Object type Range for Source Translated. Range preferred because of predictable outcome. Example of why to use this: YouTube can blacklist a university due to too many connections from one WAN IP. (Note: This is if you own a block of IP addresses)
- NEVER set Service Translated to same Service as Service Original, always use ORIGINAL or PAT Port. This could occur due to replicating a config from another manufacturer's firewall
- Good idea to NOT use firewall's Primary WAN IP (or other high priority IP in Subnet, such as your outbound email SMTP IP) for Guest network’s Outbound NAT Policy. This protects against blacklisting.

# FIREWALL SETTINGS

- Firewall Settings >>> Advanced
  - Enable Stealth Mode, Enable Randomize IP ID & Enable Decrement IP TTL for forwarded traffic.
    - KB Article Reference: <https://support.sonicwall.com/kb/sw12547>
  - Choose best “Connections” setting. There is a Help icon  you can mouse-over to view these values. If connections in ‘DPI Connections’ mode is enough, use that as it has best DPI performance. (Allocates more memory to DPI/Requires a reboot)

# BANDWIDTH MANAGEMENT

- Bandwidth Management
  - Don't enable it if you are not using it. Most people forget to adjust when their ISP speed changes
  - Use Advanced Mode (Firewall Settings >>> BWM)
  - Name Firewall >>> Bandwidth Objects so name tells you how configured
    - Example: 'BWM - P4/G00Kb/M10Mb/E1Mb/Delay'
    - Reason: GUI pages where BWM Objects are selected display nothing other than the name.

# SSL VPN

- SSL VPN >>> Server Settings:
  - Change SSLVPN Port to 443.
    - This is done to enhance the end user's experience.
    - Note: You must first change the default HTTPS Management port (443) mentioned previously
    - Note: SSLVPN terminates on the SonicWall's Interface IP(s) and cannot be changed to another IP in Interface's subnet. Note this so you can address other potential inbound NAT Policy conflicts
  - It is recommended to have a public (purchased) cert meeting the latest encryption standards. The self signed cert provided by the firewall is adequate, but will not pass PCI audits

# SECURITY SERVICES

## GAV

- Check all boxes on main screen
  - Don't forget Cloud AV
  - Note on TCP Stream:
    - If you do not enable, DPI will only scan listed protocols (HTTP, FTP, SMTP, etc.) on default port(s)

## IPS

- High/Med=Prevent+Detect
- Low=Detect
- Customize the following Categories to Prevent+Detect (+ change log redundancy as needed):
  - Backdoor, Bad-Files, Compromised-Certs, DB-Attacks, Virus, Web-Attacks
- Review other Low priority signatures and change to Prevent+Detect as needed (+ change log redundancy)

## Anti-Spyware

- Check all boxes

# SECURITY SERVICES

## Geo IP

- Turn on in either “All connections” or “Firewall Rule-based Connections” (recommended) mode depending on needs. For example, do you have a DNS server that must perform recursive lookups on a DNS server in a blocked country?
  - Enable logging
  - Consider blocking ‘Anonymous Proxy/Private IP’ and ‘All Unknown’. However, note that you may have IP addresses requiring exclusion

## Botnet Filter

- Turn on in “All connections” mode
  - Enable logging



# LOGGING

- Log >>> Name Resolution >>> Name Resolution Method:
  - Disable (None) or set to DNS
  - Point to Internal DNS servers otherwise no RFC1918 resolution (192.168.x.x, 172.16-31.x.x, 10.x.x.x)
- Log >>> Automation: : In most cases, this creates an overwhelming amount of email and can put undue strain firewall's Core0.
  - Thus, this feature is not recommended for logs. Utilize syslog to SonicWall GMS or Analyzer or send to a 3rd party Syslog collector
  - For Alerts, don't set globally here. Set specific alerts you wish to receive by email via Log >>> Settings >>> Edit the Event
    - Regardless, verify email settings are correct if doing this
    - Better: SonicWall GMS's Live Monitor feature is recommended for this as it is more efficient, will send a more detailed email alert and can send a SNMP trap as well. Up to 5 destinations, each with a different schedule
- Log >>> Settings >>>
  - Security Services >>> General: Disable 'Raw Data' (Event ID 1391) by unchecking GUI, Alert, Syslog, & Email, Click Apply
  - Network >>> NAT: Disable 'Connection NAT Mapping' (Event ID 1197) by unchecking GUI, Alert, Syslog, & Email, Click Apply
    - Note: This information can be useful. For example, if you need to determine who downloaded a pirated movie because you received a DMCA violation email that your public IP broke the law, you need to log this information to track down what private IP was associated with the public ip:port in the notice. Also note that GMS and Analyzer have a filter for this event (as well as Raw Data) so, by default, it is not written to GMS's/Analyzer's reporting database.

## LOGGING – APP CONTROL ADVANCED

- Log >>> Settings >>> Firewall >>> Application Control: Disable ‘Application Control Detection Alert’ (Event ID 1154) from GUI.
  - Don’t disable for Syslog as you need that for GMS/Analyzer reporting on Application Data Usage.
  - This change saves on-box logging and Core0 from processing the large number of events whose on-box log display provides little value in most installations.
- Global Log Redundancy Filter: Set >0.
  - Reason: for a 60 second video, 0 creates ~180 events which translate to 180 syslogs. Changing it to just 1 second reduces that down to ~38. Old default was 0, new default is 60 seconds.
  - Change the Log Redundancy filters for Web Browser and Protocols categories to 60 seconds.
  - For other categories, at least increase it to 15-20 seconds

# HIGH AVAILABILITY

- Try and always use x0, and configure its Monitoring IP addresses
  - x0 is hardcoded in SonicOS as the backup heartbeat link
  - Additionally, if no WAN interface has Monitoring IP addresses configured, it is the Secondary/Standby unit's path to Internet for GRID and License Manager communication
- The Secondary unit is never licensed automatically
  - Always login to it via one of its Monitoring IP addresses, put in the registration code and sync its licensing with MySonicWall. If both units have been properly associated in MySonicWall it will get all licensing.
- Firewall changes requiring a reboot **can easily cause an outage**
  - Reason: When a change requiring a firewall reboot is made, the "Status" shown at the bottom left-hand corner of the firewall's administration GUI changes from "Status: Ready" to "Status: Reboot...". When this happens in a HA pair, the behavior is the Standby firewall will reboot when the change is made **prior to clicking on "Status: Reboot"**. So, if you click Reboot while the Standby unit is rebooting both firewalls will be unavailable and you just brought the network down.
- Use the Virtual Mac option: This simply reduces ARP convergence time during a failover
  - HA Pair connected to the same switch: Make sure that the Switch Ports connected to the SonicWALL Interfaces have STP (Spanning Tree Protocol) disabled. Essentially STP has a real problem with our Virtual MAC being seen on multiple interfaces, and will cause a flapping effect to the firewalls.

# ADDITIONAL SECURITY ENHANCEMENTS

- Firewall Rules for Security Enhancement
  - DNS: Add Outbound Rules for DNS:
    - Deny Rule: Block all DNS queries (UDP/53) from Inside to Outside (i.e. LAN to WAN)
    - Allow Rule: Only allows DNS queries (UDP/53) to specific/sanctioned DNS servers like Google, etc.
  - SMTP: Only allow Outbound SMTP access for sanctioned email servers, block all else
  - SSH: Add Deny Rule to block all outbound SSH. When malware tries everything to get out it could try SSH which currently cannot be scanned by man-in-the-middle (DPI-SSL). DPI-SSH is a new feature in SonicOS 6.2.7
- Content Filtering – Categories to always control: Hacking/Proxy Avoidance Systems, Pay to Surf Sites, Internet Watch Foundation and Malware
  - When Ready/Where Possible, also block Not Rated. Blocking this category will cause Availability/Usability challenges. Therefore, before implementing, look at report of traffic to Not Rated sites (and IP addresses) and add sanctioned destinations to allow list or re-categorize those sites. (i.e. <http://ipaddress> is almost certainly not rated)
    - To help mitigate this, CFS 4.0 in SonicOS 6.2.6+ adds both Confirm and Passphrase bypass page options, rather than Block. Thus, could be used to mitigate this issue for N/R sites.

# ADDITIONAL SECURITY ENHANCEMENTS

- Gateway Anti-Virus Lockdown
  - On each protocol (HTTP, FTP, etc.) you can additionally block:
    - Restrict Transfer of password-protected ZIP files
    - Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)
    - Restrict Transfer of packed executable files (UPX, FSG, etc.)

NOTE: These Settings will cause Usability/Availability challenges for users



THANK YOU

The SonicWall logo features the word "SONICWALL" in a bold, sans-serif font. The "W" is stylized with a small orange swoosh underneath it. The logo is positioned at the bottom left of the slide, where two large, thin, grey curved lines converge.

SONICWALL™

March 2017