<table>
<thead>
<tr>
<th>Check ID</th>
<th>Title</th>
<th>Rule ID</th>
<th>Vuln ID</th>
<th>Severity</th>
<th>Class</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>NET0812</td>
<td>Two NTP servers are not used to synchronize time.</td>
<td>SV-41498r1_rule</td>
<td>V-23747</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0900</td>
<td>SNMP traffic does not use loopback address.</td>
<td>SV-15347r2_rule</td>
<td>V-14675</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET1675</td>
<td>SNMP privileged and non-privileged access.</td>
<td>SV-3043r2_rule</td>
<td>V-3043</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0422</td>
<td>Key expiration exceeds 180 days.</td>
<td>SV-15301r2_rule</td>
<td>V-14667</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0396</td>
<td>Alerts must remain until acknowledged.</td>
<td>SV-15281r1_rule</td>
<td>V-14655</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1647</td>
<td>The network element must not allow SSH Version 1.</td>
<td>SV-15459r2_rule</td>
<td>V-14717</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0812</td>
<td>Two NTP servers are not used to synchronize time.</td>
<td>SV-41497r1_rule</td>
<td>V-23747</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1646</td>
<td>SSH login attempts value is greater than 3.</td>
<td>SV-15458r2_rule</td>
<td>V-5613</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0405</td>
<td>Call home service is disabled.</td>
<td>SV-38003r2_rule</td>
<td>V-28784</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1639</td>
<td>Management connection does not timeout.</td>
<td>SV-15453r2_rule</td>
<td>V-3014</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0965</td>
<td>Devices not configured to filter and drop half-open connections.</td>
<td>SV-15437r4_rule</td>
<td>V-5646</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET1640</td>
<td>Management connections must be logged.</td>
<td>SV-3070r2_rule</td>
<td>V-3070</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0410</td>
<td>BGP sessions are not restricted.</td>
<td>SV-15299r1_rule</td>
<td>V-3035</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0440</td>
<td>More than one emergency account is defined.</td>
<td>SV-30085r3_rule</td>
<td>V-3966</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0340</td>
<td>Login banner is non-existent or not DOD approved.</td>
<td>SV-3013r2_rule</td>
<td>V-3013</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET1629</td>
<td>The auxiliary nor is not disabled.</td>
<td>SV-7365r2_rule</td>
<td>V-7011</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NX-OS</td>
</tr>
<tr>
<td>NET-IPV6</td>
<td>IPv6 Loopback ADDR is not blocked by the enclave.</td>
<td>SV-15402r1_rule</td>
<td>V-14696</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS</td>
</tr>
<tr>
<td>NET-SRVR</td>
<td>ACLs must restrict access to server VLANs.</td>
<td>SV-20061r2_rule</td>
<td>V-18522</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS</td>
</tr>
<tr>
<td>NET1623</td>
<td>Authentication required for console access.</td>
<td>SV-28747r3_rule</td>
<td>V-4582</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0726</td>
<td>Identification support is enabled.</td>
<td>SV-5616r2_rule</td>
<td>V-5616</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0340</td>
<td>Login banner is non-existent or not DOD approved.</td>
<td>SV-3013r2_rule</td>
<td>V-3013</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1640</td>
<td>Management connections must be logged.</td>
<td>SV-15455r2_rule</td>
<td>V-3070</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0390</td>
<td>The IDS or FW is not configured to alarm the admin.</td>
<td>SV-31761r1_rule</td>
<td>V-3176</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0405</td>
<td>Call home service is disabled.</td>
<td>SV-38003r2_rule</td>
<td>V-28784</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0391</td>
<td>FA is not informed of critical alerts.</td>
<td>SV-15274r1_rule</td>
<td>V-14648</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0400</td>
<td>Interior routing protocols are not authenticated.</td>
<td>SV-15291r2_rule</td>
<td>V-3034</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET-MCAS</td>
<td>PIM neighbor filter is not configured.</td>
<td>SV-40315r1_rule</td>
<td>V-30578</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0440</td>
<td>More than one emergency account is defined.</td>
<td>SV-15469r3_rule</td>
<td>V-3965</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET600</td>
<td>Passwords are viewable when displaying the config.</td>
<td>SV-41499r2_rule</td>
<td>V-3062</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1970</td>
<td>PAT is vulnerable to DNS cache poisoning.</td>
<td>SV-30841r1_rule</td>
<td>V-25037</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS, Cisco FWSM v2, Cisco PIX v6</td>
</tr>
<tr>
<td>NET0927</td>
<td>RFC1918 addresses are not blocked.</td>
<td>SV-15394r2_rule</td>
<td>V-14692</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0927</td>
<td>RFC 1918 addresses are not blocked.</td>
<td>SV-15393r2_rule</td>
<td>V-14692</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS</td>
</tr>
<tr>
<td>NET0740</td>
<td>HTTP server is not disabled.</td>
<td>SV-41468r1_rule</td>
<td>V-3085</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0230</td>
<td>Network element is not password protected.</td>
<td>SV-3012r2_rule</td>
<td>V-3012</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0966</td>
<td>Control plane protection is not enabled.</td>
<td>SV-21168r2_rule</td>
<td>V-19188</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET0230</td>
<td>Network element is not password protected.</td>
<td>SV-3012r2_rule</td>
<td>V-3012</td>
<td>CAT I</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco FWSM v2, Cisco PIX v6</td>
</tr>
<tr>
<td>NET0400</td>
<td>Interior routing protocols are not authenticated.</td>
<td>SV-15290r2_rule</td>
<td>V-3034</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET1629</td>
<td>The auxiliary port is not disabled.</td>
<td>SV-15446r2_rule</td>
<td>V-7011</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0398</td>
<td>FW acknowledge messages must be recorded.</td>
<td>SV-15320r1_rule</td>
<td>V-14656</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco PIX v7/8, Cisco PIX v6</td>
</tr>
<tr>
<td>NET0580</td>
<td>Password required on the JUNOS diagnostic port.</td>
<td>SV-4583r1_rule</td>
<td>V-4583</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
<tr>
<td>NET1624</td>
<td>The console port does not timeout after 10 minutes.</td>
<td>SV-3967r2_rule</td>
<td>V-3967</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS, Cisco FWSM v2, Cisco PIX v6</td>
</tr>
<tr>
<td>NET0992</td>
<td>The management interface does not have an ACL.</td>
<td>SV-2020r1_rule</td>
<td>V-17822</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>NET0375</td>
<td>Firewalls is not configured to protect the network.</td>
<td>SV-3156r1_rule</td>
<td>V-3156</td>
<td>CAT II</td>
<td>Unclass</td>
<td>Cisco IOS, Cisco NFOS, Cisco FWSM v2, Cisco PIX v6</td>
</tr>
<tr>
<td>NET1020</td>
<td>Interface ACL deny statements are not logged.</td>
<td>SV-15475r3_rule</td>
<td>V-3000</td>
<td>CAT III</td>
<td>Unclass</td>
<td>Juniper JunOS</td>
</tr>
</tbody>
</table>
NET-TUNL: Teredo is not blocked by filtering UDP port 3544

SV-16075r4_rule  V-15294  CAT I  Unclass  Juniper JunOS

NET0377: Firewall has unnecessary services enabled.

SV-30541r1_rule  V-3054  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

SV-15298r1_rule  V-3035  CAT II  Unclass  Cisco IOS

NET0950: uRPF strict mode or ACL not enabled on egress interface.

SV-15423r2_rule  V-3164  CAT I  Unclass  [Cisco IOS, Cisco NX-OS]

NET0965: Devices not configured to filter and drop half-open connections.

SV-5646r1_rule  V-5646  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0730: The finger service is not disabled.

SV-15306r2_rule  V-3079  CAT III  Unclass  Juniper JunOS

SV-5402r1_rule  V-7009  CAT I  Unclass  Cisco IOS

SV-30542r1_rule  V-7009  CAT I  Unclass  Cisco IOS

NET0433: The device is not authenticated using a AAA server.

SV-16259r2_rule  V-15432  CAT II  Unclass  Cisco IOS

NET1639: Management connection does not timeout.

SV-3275r2_rule  V-3014  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0813: NTP messages are not authenticated.

SV-41501r1_rule  V-14671  CAT II  Unclass  Juniper JunOS

NET0901: Netflow traffic is not using loopback address.

SV-15349r2_rule  V-14676  CAT III  Unclass  Cisco IOS

NET0728: DHCP service is not disable on premise

SV-5617r1_rule  V-5617  CAT III  Unclass  Cisco IOS

NET0781: Gratuitous ARP must be disabled.

SV-5618r2_rule  V-5618  CAT III  Unclass  Cisco IOS

NET0433: The device is not authenticated using a AAA server.

SV-16259r2_rule  V-15432  CAT II  Unclass  Juniper JunOS

NET0924: IPv4 Link-local address is not blocked

SV-15388r2_rule  V-4690  CAT I  Unclass  Juniper JunOS

NET0923: IPv4 Loopback address is not blocked

SV-15385r2_rule  V-4689  CAT I  Unclass  Juniper JunOS

NET1646: SSH login attempts value is greater than 3.

SV-5613r2_rule  V-5613  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-IPV6-I: IPv6 Unspecified ADDR is not blocked

SV-15406r1_rule  V-14696  CAT I  Unclass  Juniper JunOS

NET0902: FTP/HTTPS traffic does not use loopback address.

SV-15353r3_rule  V-14677  CAT III  Unclass  Juniper JunOS

NET0950: uRPF strict mode or ACL not enabled on egress interface.

SV-15424r2_rule  V-3164  CAT I  Unclass  Juniper JunOS

NET0722: The PAD service is enabled.

SV-5614r2_rule  V-5614  CAT III  Unclass  Cisco IOS

NET0740: HTTP server is not disabled

SV-41470r1_rule  V-3085  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-SRVR ACLs do not protect against compromised servers

SV-20062r1_rule  V-18523  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0740: HTTP server is not disabled.

SV-41467r1  V-3085  CAT II  Unclass  Cisco IOS

NET1647: The network element ust not allow SSH Version 1.

SV-15460r2_rule  V-14717  CAT II  Unclass  Cisco IOS

NET-NAC-SwitchPort does not shutdown on a violation

SV-20109r1_rule  V-18565  CAT III  Unclass  Cisco IOS

NET1665: Using default SNMP community names.

SV-3210r2_rule  V-3210  CAT I  Unclass  Juniper JunOS

NET-IPV6-I: IPv6 Site Local Unicast Addresses are not blocked

SV-15400r1_rule  V-14694  CAT I  Unclass  Juniper JunOS

NET-IPV6-I: IPv6 Jumbo payload hop by hop is not dropped

SV-20551r1_rule  V-18815  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1638: Management connections must be secured by FIPS 140-2.

SV-154513_rule  V-3069  CAT II  Unclass  Cisco IOS

NET1624: The console port does not timeout after 10 minutes.

SV-15444r2_rule  V-3967  CAT II  Unclass  Cisco IOS

NET0813: NTP messages are not authenticated.

SV-41500r1_rule  V-14671  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0422: NET0422 - Key expiration exceeds 180 days.

SV-15301r2_rule  V-14667  CAT III  Unclass  Juniper JunOS

NET0897: Authentication traffic does not use loopback address

SV-16092r2_rule  V-14672  CAT III  Unclass  Juniper JunOS

NET-IPV6-I: IPv6 routers are not configured with CEF enabled

SV-15425r1_rule  V-14705  CAT II  Unclass  Cisco IOS

NET0812: Two NTP servers are not used to synchronize time.

SV-41499r1_rule  V-23747  CAT III  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0770: IP Source Routing is not disabled on all routers.

SV-15316r2_rule  V-3081  CAT II  Unclass  Cisco IOS

NET0742: FTP server is not disabled

SV-15312r1_rule  V-14668  CAT II  Unclass  Juniper JunOS

NET1636: Management connections must require passwords.

SV-3175r3_rule  V-3175  CAT I  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1660: An insecure version of SNMP is being used.

SV-3196r2_rule  V-3196  CAT I  Unclass  Juniper JunOS

NET1639: Management connection does not timeout.

SV-15454r2_rule  V-3014  CAT II  Unclass  Juniper JunOS

NET0820: DNS servers must be defined for client resolver.

SV-3053r1_rule  V-3020  CAT III  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1647: The network element must not allow SSH Version 1.

SV-15461r2_rule  V-14717  CAT II  Unclass  Juniper JunOS

NET-IPV6-I: IPv6 Site Local Unicast Addresses are not blocked

SV-15399r1_rule  V-14694  CAT I  Unclass  [Cisco IOS, Cisco NX-OS]

NET1646: SSH login attempts value is greater than 3.

SV-28745r2_rule  V-5613  CAT II  Unclass  Juniper JunOS

NET0966: Control plane protection is not enabled.

SV-21167r2_rule  V-19188  CAT II  Unclass  Cisco IOS

NET0897: Authentication traffic does not use loopback address.

SV-16091r2_rule  V-14672  CAT III  Unclass  Cisco IOS

NET-NAC-C NET-NAC-009

SV-42190r2_rule  V-5626  CAT I  Unclass  Cisco IOS

NET0720: TCP and UDP small server services are not disabled.

SV-3078r2_rule  V-3078  CAT III  Unclass  Cisco IOS

NET1675: SNMP privileged and non-privileged access.

SV-3043r2_rule  V-3043  CAT II  Unclass  Juniper JunOS
An insecure version of SNMP is being used.

The network element must log all messages except debugging.

IPv4 Loopback address is not blocked

The VLAN1 is being used for management traffic.

Emergency account privilege level is not set.

Teredo is not blocked by filtering UDP port 3544

LAN addresses are not protected from the public.

Maximum hop limit is less than 32

Management connections must require passwords.

Management connections must only allow SNMP read access.

Network element must log all messages except debugging.

Authentication required for console access.

Emergency account privilege level is not set.

The network element must log all messages except debugging.

Network element is not password protected.

Firewall Admin will be logged.

FTP/TFTP traffic does not use loopback address.

BSDr commands are not disabled.

IPv4 Loopback address is not blocked

IPv4 Loopback address is not blocked

IPv4 Loopback address is not blocked

LAN addresses are not protected from the public.

Using default SNMP community names.

Access switchports are assigned to the native VLAN

VLAN 1 traffic traverses across unnecessary trunk

Invalid group used for source specific multicast

Invalid group used for source specific multicast

IPv6 Site Local Unicast ADDR must not be defined

Teredo is not blocked by filtering UDP port 3544

The VLAN1 is being used for management traffic.
NET-IPV6-t  The 6-to-4 router is not filtering protocol 41  
SV-40454r1_rule  V-30660  CAT II  Unclass  Cisco IOS

NET0910  Perimeter is not compliant with DOD Instr. 8551.1  
SV-5731r1_rule  V-5731  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0898  Syslog traffic is not using loopback address  
SV-15341r2_rule  V-14673  CAT III  Unclass  Juniper JunOS

NET0901  Netflow traffic is not using loopback address.  
SV-15350r2_rule  V-14676  CAT III  Unclass  Juniper JunOS

NET0386  Alerts generated at 75% log storage capacity.  
SV-15277r2_rule  V-14846  CAT III  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-IPV6-t  Maximum hop limit is less than 32  
SV-40389r1_rule  V-30617  CAT III  Unclass  Cisco IOS

NET1021  The network element must log all messages except debugging  
SV-15477r2_rule  V-4584  CAT III  Unclass  Juniper JunOS

NET0340  Login banner is non-existent or not DOD approved  
SV-3013r2_rule  V-3013  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-IPV6-t  IPv4 Interfaces in NAT-PAT receive IPv6  
SV-16078r1_rule  V-15296  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-TUNL-L2TP is terminated in the private network.  
SV-3982r2_rule  V-3982  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0366  Firewall inspection is not performed adequately  
SV-15269r1_rule  V-14643  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET-IPV6-t  IPv6 Site Local Unicast ADDR must not be defined  
SV-15397r1_rule  V-14693  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0392  FW alert not written to remote console.  
SV-15275r1_rule  V-14649  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1645  SSH session timeout is not 60 seconds or less.  
SV-28744r2_rule  V-5612  CAT II  Unclass  Juniper JunOS

NET-IPV6-t  IPv6 Loopback ADDR is not blocked by the enclave  
SV-15403r1_rule  V-14695  CAT I  Unclass  Juniper JunOS

NET-TUNL-Teredo is not blocked by filtering UDP port 3544  
SV-16075r4_rule  V-15294  CAT I  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0240  Devices exist with standard default passwords  
SV-3143r2_rule  V-3143  CAT I  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1636  Management connections must require passwords.  
SV-28748r3_rule  V-3175  CAT I  Unclass  Juniper JunOS

NET0903  Loopback address is not used as the iBGP source IP.  
SV-15360r2_rule  V-14681  CAT III  Unclass  Juniper JunOS

NET0820  DNS servers must be defined for the client resolver.  
SV-15331r1_rule  V-3020  CAT III  Unclass  Juniper JunOS

NET1970  PAT is vulnerable to DNS cache poisoning  
SV-30843r1_rule  V-25037  CAT I  Unclass  Juniper JunOS

NET0790  IP directed broadcast is not disabled.  
SV-3083r2_rule  V-3083  CAT I  Unclass  Cisco IOS

NET0949  Cisco Express Forwarding (CEF) not enabled on supported devices.  
SV-5645r3_rule  V-5645  CAT II  Unclass  Cisco IOS

NET0813  NTP messages are not authenticated.  
SV-15327r2_rule  V-14671  CAT II  Unclass  Cisco IOS

NET0965  Devices not configured to filter and drop half-open connections.  
SV-15435r3_rule  V-5646  CAT II  Unclass  Cisco IOS

NET1020  Interface ACL deny statements are not logged.  
SV-15474r3_rule  V-3000  CAT III  Unclass  Cisco IOS

NET0408  BGP must authenticate all peers.  
SV-41556r2_rule  V-31285  CAT II  Unclass  Juniper JunOS

NET0820  DNS servers must be defined for client resolver.  
SV-15330r2_rule  V-3020  CAT III  Unclass  Cisco IOS

NET0894  Network element must only allow SNMP read access.  
SV-30086r3_rule  V-3969  CAT II  Unclass  Cisco IOS

NET0441  Emergency account privilege level is not set.  
SV-16261r2_rule  V-15434  CAT I  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0395  Audit record must display violation  
SV-15279r1_rule  V-14653  CAT III  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1660  An insecure version of SNMP is being used.  
SV-3196r2_rule  V-3196  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET0903  Loopback address is not used as the iBGP source IP.  
SV-15359r2_rule  V-14681  CAT III  Unclass  Cisco IOS

NET0240  Devices exist with standard default passwords.  
SV-3143r2_rule  V-3143  CAT I  Unclass  Juniper JunOS

NET0744  BSDr commands are not disabled.  
SV-15314r2_rule  V-14669  CAT II  Unclass  Cisco IOS

NET0440  More than one emergency account is defined.  
SV-15469r3_rule  V-3966  CAT II  Unclass  [Cisco PIX v7/8 - ASA v8 - FWSM v3/4, Cisco IOS, Cisco FWSM v2, Cisco PIX v6]

NET1665  Using default SNMP community names.  
SV-3210r2_rule  V-3210  CAT I  Unclass  Cisco IOS

NET1624  The console port does not timeout after 10 minutes.  
SV-15445r2_rule  V-3967  CAT II  Unclass  Juniper JunOS

NET-IPV6-t  IPv6 Unspecified ADDR is not blocked  
SV-15405r1_rule  V-14696  CAT I  Unclass  [Cisco IOS, Cisco NX-OS]

NET1800  IPSec VPN is not configured as a tunnel type VPN.  
SV-3008r1_rule  V-3008  CAT II  Unclass  Cisco IOS

NET1800  IPSec VPN is not configured as a tunnel type VPN.