Incident Report

The Incident was reported on December 2nd, when the End User suspected spurious activity on the Collector Server. It was communicated through the Support Portal, ticket number GBL-128-51113.

The investigation of the incident went through the following steps:

- Our engineers performed analysis on the compromised server via a TeamViewer connection;
- Upon identification of malware, the server was disconnected from the Internet;
- A sophisticated analysis was conducted on the samples of malware sent by the End User.

Following, the results of the analysis:

The file "Gqwdpfieg.gif", found in the profile “Mwoo”, installs a service on the machine and puts itself in autostart. Its hash (33B6B5572141B69A372162E344DF170F7A5F59BC) is not in the VirusTotal database.

The file "Gqwdpfieg.gif" installs itself as a service and tries to contact the host 1.wan567.com, registered to:

```
Domain Name: WAN567.COM
Creation Date: 2012-05-21 07:08:00Z
Registrar Registration Expiration Date: 2014-05-20 23:08:00Z
Registrar: ENOM, INC.
Registrant Name: AI SHIDA
Registrant Organization: AI SHIDA
Registrant Street: SHANXISHENGXIANSHIGAOXINQUTIANQUANKEJI
Registrant City: XIAN
Registrant State/Province: SHAXI
Registrant Postal Code: 710000
Registrant Country: CN
Admin Name: AI SHIDA
Admin Organization: AI SHIDA
Admin Street: SHANXISHENGXIANSHIGAOXINQUTIANQUANKEJI
Admin City: XIAN
Admin State/Province: SHAXI
Admin Postal Code: 710000
Admin Country: CN
Admin Phone: +86.13251821132
Admin Phone Ext:
Admin Fax: +86.103323192
Admin Fax Ext:
Admin Email: 369700092@QQ.COM
Tech Name: AI SHIDA
Tech Organization: AI SHIDA
Tech Street: SHANXISHENGXIANSHIGAOXINQUTIANQUANKEJI
Tech City: XIAN
Tech State/Province: SHAXI
Tech Postal Code: 710000
Tech Country: CN
Tech Phone: +86.13251821132
Tech Phone Ext:
Tech Fax: +86.103323192
```

Tech Fax Ext:
Tech Email: 369700092@QQ.COM
Name Server: NS103.DNSEVER.COM
Name Server: NS11.DNSEVER.COM
Name Server: NS97.DNSEVER.COM

Connection to Domain Name and Port used by the malware is impossible at the moment; the service was probably stopped on their side.

Of the other files that are part of the malware installed, we found tools for DDOS (Distributed Denial of Service), Trojans, and others.

About the folders with root C:\Users that we analyzed:

- mwoo - is not a real user profile, but it is where the file "Gqwdpfieg.gif" has been dropped.
- 5758 – is the home folder for a different user; without the SAM file in SYSTEM32\Config we cannot confirm this.
- Administrator – in the Registry entries of this user have been found parameters belonging to Camfrog; this means that Camfrog has been started at least once.

Without a forensic copy of the hard drive of the server, it is impossible for us to extract further information or to determinate the date of the incident.

Conclusions

There is no clear evidence of exfiltration of files related to from the compromised server. Anyway, the security of the server is irremediably compromised.

Next Steps

The next steps to restore the system are as following:

1. Setup the network appropriately, with the needed network appliances (see Paragraph 3)
2. Backup all the data. You will need to make a copy of:
   - On the Collector: C:\RCS
   - On the Master Node: C:\RCS

   Save the copies on an external drive, and make sure you put it in a safe place. <u>This backup is necessary to restore of the system without losing agents or evidence.</u>
3. Completely format both servers, Collector and Master Node.
4. Install Windows Server 2008R2 SP1 on both Collector and Master Node.
5. Install Team Viewer on both Collector and Master Node.
6. Perform hardening on both Windows Servers (remote support is available for this task)
7. Install latest version of software (remote support is available for this task)
8. Restore the backed up files (remote support is available for this task)
9. Check the health of the newly installed System (remote support is available for this task)

Please notice that during this process no Agents or evidence will be lost.

Servers must be dedicated, no other use is allowed; in particular, the system shall not be configured as a network gateway.

No 3rd party software shall be installed, if not previously agreed before. 3rd party software may impact the correct functionality of the system or degrade its security.

FOR NO REASON ANTIVIRUS SOFTWARE SHALL BE INSTALLED ON THE SERVERS.

Any remote access tool (Remote Desktop, TeamViewer) shall be enabled only upon request from our support, and only for the time needed. When remote support is enabled, a person from End User must attend all the operations done by our engineers.

Network Configuration

The security of the whole System depends mainly on the correct Network Configuration, which includes Firewall and Switch.

To comply with minimum network security requirements, in this section we suggest equipment and configuration that should be adopted.

Firewall

System Requirements

The following must be present:

1. Support for VPN connection client to site (SSL or IPSEC)
2. Stateful throughput of 1 Gbps
3. IMIX performance of 235 Mbps
4. Maximum connections of 225000
5. VPN throughput of 300 Mbps

Suggested Hardware Specifications

Below you can find a recommended hardware configuration for firewall.

SonicWall NSA 2400MX Network Security Appliance
IPSEC VPN Connections Client to Site: Up to 10
Stateful Throughput: 775 Mbps
IMIX Performance: 235 Mbps
Maximum Connections: 225000
VPN Throughput: 300 Mbps

Switch

System Requirements

The following must be present:

1. 24 ports
2. Support for 10/100/1000 Mbps

Suggested Hardware Specifications

Below you can find a recommended hardware configuration for the switch.

Dell PowerConnect 2800
Ports : 24 at least
Speed: 10/100/1000 Mbps

VLANs Configuration on Switch

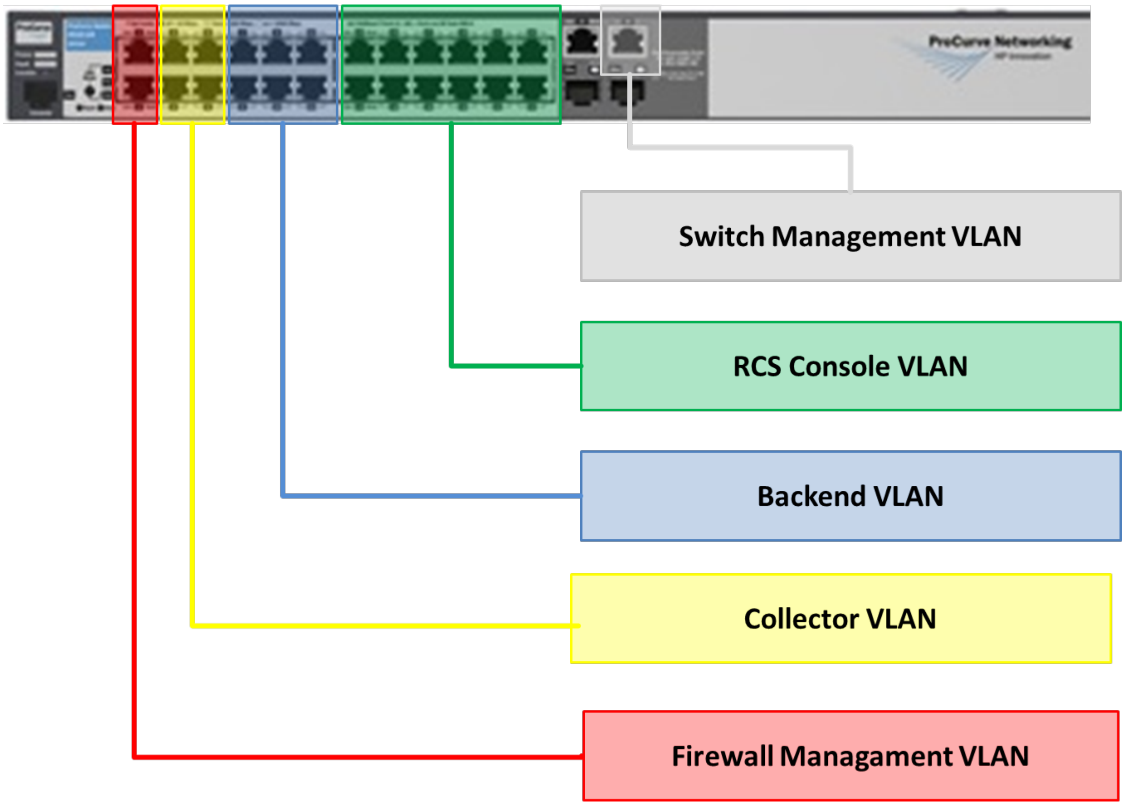
The environment requires 5 VLANs on a switch.

These VLANs create different logical LAN for each component and for devices management.

On the switch you can create there VLANs:

- Backend VLAN
- Collector VLAN
- Console VLAN
- Firewall Management VLAN
- Switch Management VLAN

The assigned ports on the switch for each VLAN could be 2 or more, depending on the architecture.


ProCurve Networking
Switch Management VLAN
RCS Console VLAN
Backend VLAN
Collector VLAN
Firewall Managament VLAN

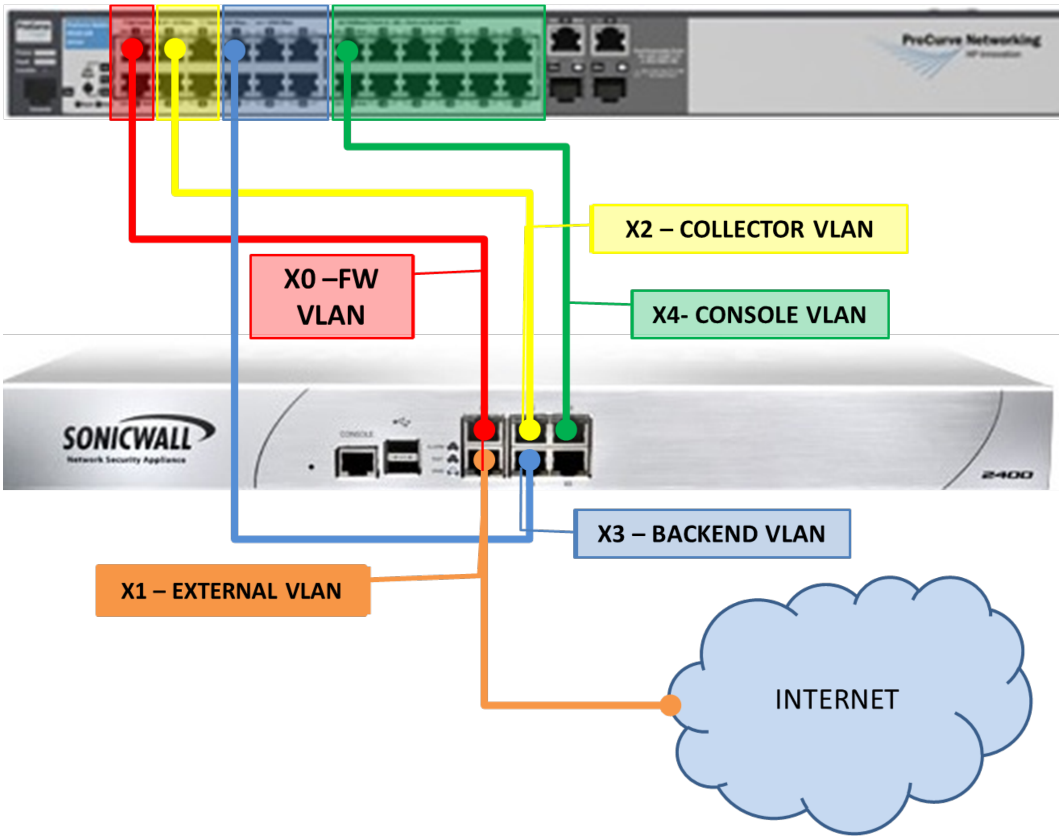
Firewall → Switch Interconnection

The firewall is used to regulate communication between VLANs.

Five zones are configured on the firewall:

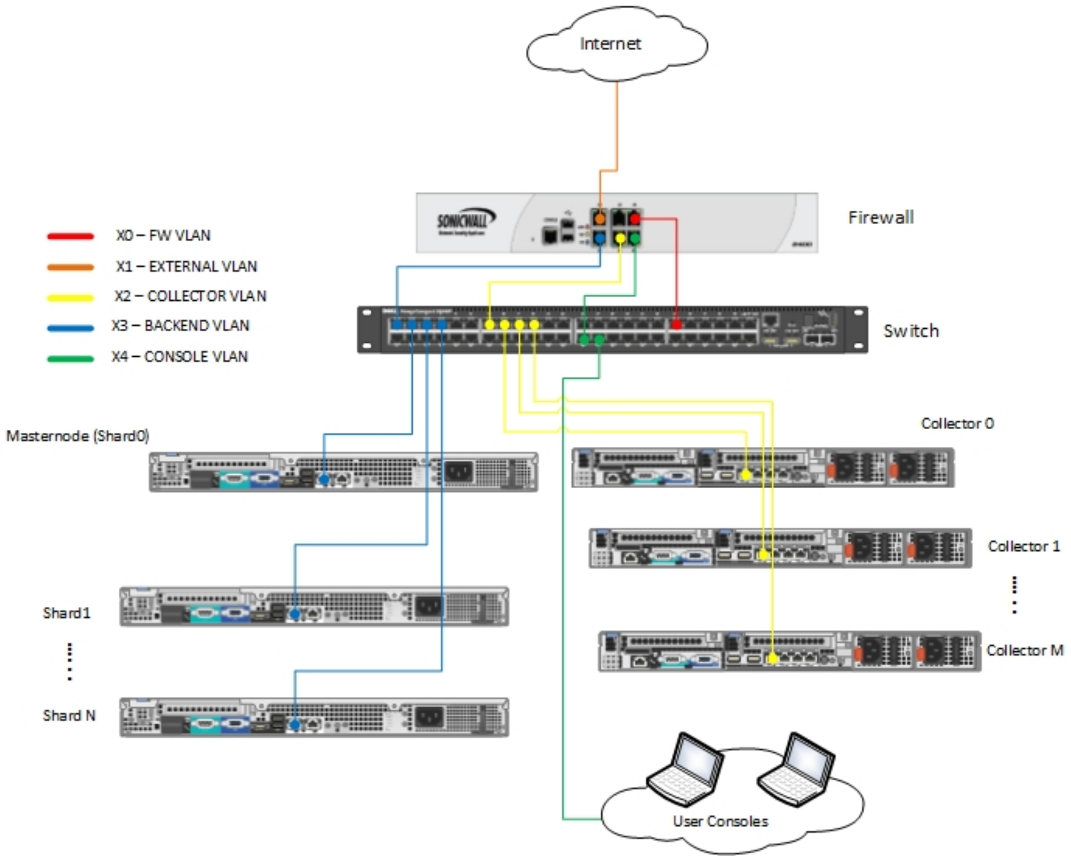
- Backend VLAN
- Collector VLAN
- Console VLAN
- Firewall Management VLAN
- External VLAN (Internet)

Zones on the firewall and VLANs on the switch must be connected according to the picture below.



Hardware Interconnection Schema

Following is represented the whole system architecture with its interconnections. As described in the picture, final infrastructure may include additional Collectors and Shards.



Firewall Rules Setup

The following rules must be implemented on the firewall.

Table’s colors reflect the colors used in previous pictures.

Source	Destination	Service	Protocol	Port
Backend	Any	DNS	UDP	53
Backend	Any	NTP	UDP	123
Backend	TNI	HTTPS	TCP	443
Backend	Collector	HTTPS	TCP	443
Backend	Collector	HTTP	TCP	80
Console	Any	HTTPS	TCP	443
Console	Any	HTTP	TCP	80
Console	Any	DNS	UDP	53
Console	Any	ICMP	ICMP	
Console	Collector	RDP	TCP	3389
Console	Backend	RDP	TCP	3389
Console	Backend	HTTPS	TCP	443
Console	Backend	TCP_444	TCP	444
Collector	Any	DNS	UDP	53
Collector	Any	HTTP	TCP	80
Collector	Any	HTTPS	TCP	443
Collector	Any	NTP	UDP	123
Collector	Backend	HTTPS	TCP	443
Anonymizer(s)	Collector	HTTP	TCP	80