Managed Security Appliances

Monitoring/Management Station

The ***"MonMan"*** station is a small device running a Linux server plus a small number of programs that allows the monitoring and proactive management of firewalls, routers, switches and other security and network devices which allow local and/or remote console access (command-line and/or VNC/Terminal Services/Citrix/etc. based).

MonMan allows the managed appliance to:

- use it as a syslog server; any syslog events will then be securely (via VPN) forwarded to a central ESM server maintained by xDefenders for management and alert purposes
- use it as a TFTP server; this allows the managed appliance to store configuration and run images and fast restore both after a failure
- use it as a SNMP trap destination (future)
- trap net flow statistics for bandwidth monitoring and analysis

MonMan allows xDefenders to:

- access the managed appliance on the console port (via the serial interface)
- access the managed appliance via ssh or telnet via a secure channel (SSH or VPN)
- automatically pull configuration for backup purposes

Deployment requirements:

- outside the customer firewall, ie. needs separate externally available IP address
- connected to managed appliance via serial cable (only one connection is available)
- customer must allow ping, SNMP and ssh (or telnet) to managed appliance

Total Solution:

We are providing a Managed Firewall Service that consists of the Cisco ASA or FortiGate, our MonMan and ESM systems. Taken together, this gives you professional, proactive network security management and monitoring, and compliance.

Your ASA is sending syslog data to our MonMan on a regular basis. Our MonMan regularly sends this data to our central ESM in Rochester. Our ESM provides us with a Daily Report showing alerts that are "over threshold" and we monitor, investigate and react.

In some rare cases, we will change the firewall rules accordingly or recommend other action from your part, to protect your network.

We are capturing what the ASA is programmed to send to the ESM (via MonMan). Since we manage the ASA, we are sending all syslog messages with severity levels 1 – 3.

Additionally, we are logging messages 605004, 606001, 606002, 611103, and 502103 (they all record login/logout events), but NOT 106014,
313001, and 313008 (they deal with menial events).

MonMan captures net-flow statistics. This can be used for bandwidth usage monitoring, trouble shooting and planning purposes. The MonMan can send this raw data to a NetFlow Analyzer Management System for reporting. xDefenders provides such an appliance.

Sample Reporting:

Sample Compliance Reporting for Log-ins, Log-Outs:

```
>      ------------------------------------------------------------
>      Host '1.2.3.4'
> => Yesterday's successful logons

>      ------------------------------------------------------------
>      Host 'monman.customer.com'

> => Yesterday's successful logons
> 2007-12-09 06:26:19   su[8197]: Successful su for nobody by root
> 2007-12-09 06:26:19   su[8200]: Successful su for nobody by root
> 2007-12-09 06:26:20   su[8202]: Successful su for nobody by root
```

The ESM (our central syslog management server in Rochester) creates a daily report for our CISSP staff to review. That looks like this:

```
 This email may contain several reports:
>
>  - General overview for the day and the past three days
>  - Compliance report: Successful logons for yesterday
>  - Compliance report: Unsuccessful logons for yesterday
>  - Compliance report: Logoffs for yesterday
>  - Compliance report: Object Changes for yesterday
>  - Compliance report:  IPS Activity for yesterday
>
> Statistics for group 'Customer':
>       ----------------------------------------------------------
>       Host '1.2.3.4'
>
> => Total events
> Total     : Value
> Today     :   38 *
> Yesterday : 1441 **************************************************
> Two days a: 1086 ***************************************
> Three days: 1869
************************************************************************
```

Managed Services include:

- Appliance – Design, Deploy, Manage, Monitor, Maintain
- Hardware, software and services
- Pre-Installed Configurations
- Turnkey Installation and fine-tuning of Rules
- Rule changes will be completed within 4 hours maximum
- Escalation Plan Developed with I/T Staff.
- Online Documentation, Web Interface
- Technical phone and email support
- Databases updated, automatically
- Secure SSH connection to/from xDefenders Security Operations Center
- OS and Applications patched, enhanced, remotely
- Weekly local and remote backups
- Hardware maintenance is next day overnight, replacement
- 1 Year Warranty from date of shipment
- NOC and SOC services and expertise is available
- Monday – Friday 8:30 am to 7 pm is standard support
- Optional 24x7 management and monitoring

xDefenders provides CISSP support for these Security Appliances: Cisco, Fortigate, Sonicwall and its own DefenderWall.

xDefenders provides a full range of Professional Compliance Services.

Jeff Thon, VP
xDefenders, inc.
1100 Pittsford Victor Rd
Pittsford, NY 14534
585-385-2770
fax 385-3511

http://www.xdefenders.com