June 22, 2010

Deep Packet Inspection and Application Classification with VortiQa Software

Basem Barakat
Senior Systems Engineer Software Products
Agenda

► Why deep packet inspection (DPI) is needed
► What should be inspected during a given DPI
► DPI deployment scenarios: intrusion detection system (IDS) versus intrusion prevention system (IPS)
► DPI with VortiQa software
► Freescale solution-centric approach offers DPI turnkey solution
Why Deep Packet inspection (DPI) Is Needed?
Statement of the Problem: DOS Attacks

► Denial of Service
  • Attacker generates unusually large volume of requests, overwhelming your server
  • Legitimate users are denied access
  • Can last from a few minutes to several days

► DOS Topology
  • Exploit a bug in TCP/IP implementation
  • Exploit a shortcoming in the TCP/IP protocol itself

► DOS Implementations
  • Brute-force
  • *Ping of Death*
  • *Smurf*
  • *SYN Flood*
  • *Teardrop*
  • ..... And several others

---

Smurf Attack

Attacker broadcasts echo request source address is spoofed to be target's address

many echo replies are received by the target, since most machines on the amplifier network respond to the broadcast
Statement of the Problem: Code Injection Attacks

Code Injection Attack

- Code injection is the exploitation of a bug in a given application running on a host or server node resulting in getting the host computer to execute unauthorized or invalid code.
- Code injection aim of the attack to alter the course of execution and again access and ultimately control the target node.

Code Injection Implementation

- Shell code injection
- SQL injection
- HTML script injection
- Include file injection

Buffer Overruns C / C++

- void function(char *p)
  { char buff[16];
    ...
    strcpy(buff,p); ...
  }

Integer Overflow C/C++

- void func(char *b1, size_t c1, char *b2, size_t c2)
  { const size_t MAX = 48;
    if (c1 + c2 > MAX) return;
    char *pBuff = new char[MAX];
    memcp(pBuff,b1,c1);
    memcp(pBuff+c1,b2,c2); }

Security Gateway Network Deployment Modes

**Central Security Management Center**
- Central Firewall Policy Management Server

**Enterprise Network**
- Firewall
- Web Server
- Confidential Data
- Access Control Lists
- Marketing Users
- Other Internal Users
- Finance Users
- Marketing User 1 - Policies
  - Allow access to sales server
  - Allow remote access
  - Allow access to web server
  - Deny access to finance server
  - Deny access to confidential data

**Home Office**
- VortiQa Software Firewall
- TELECOMMUTER
- VortiQa Software Firewall
- Malicious Hackers

**Internet**
- Email Server
- App Server
- EDI Server

**Central Services**
- Confidential Data

**Finance Subnet**
- Finance User Group
  - Allow access to finance servers
  - Deny access to marketing servers
  - Deny access to web server
  - Allow access to confidential data

**Marketing Subnet**
- Marketing Users

**Access Control Lists**
- Marketing User 1 - Policies
  - Allow access to sales server
  - Allow remote access
  - Allow access to web server
  - Deny access to finance server
  - Deny access to confidential data

**Other Internal Users**
- Finance Users
- Marketing Users
- Marketing User 1 - Policies

**Finance User Group**
- Allow access to finance servers
- Deny access to marketing servers
- Deny access to web server
- Allow access to confidential data

**Central Firewall Policy Management Server**
- Central Security Management Center

**Telecommuter**
- VortiQa Software Firewall

**CENTRAL SECURITY MANAGEMENT CENTER**
- Central Firewall Policy Management Server

**INTERNET**
- Email Server
- App Server
- EDI Server

**Central Services**
- Confidential Data

**MARKETING SUBNET**
- Marketing Users
- Marketing User 1 - Policies

**FINANCE SUBNET**
- Finance Users
- Finance User Group
- Marketing User 1 - Policies

**Access Control Lists**
- Marketing User 1 - Policies
  - Allow access to sales server
  - Allow remote access
  - Allow access to web server
  - Deny access to finance server
  - Deny access to confidential data

**Finance User Group**
- Allow access to finance servers
- Deny access to marketing servers
- Deny access to web server
- Allow access to confidential data

**Central Firewall Policy Management Server**
- Central Security Management Center

**Telecommuter**
- VortiQa Software Firewall

**CENTRAL SECURITY MANAGEMENT CENTER**
- Central Firewall Policy Management Server

**INTERNET**
- Email Server
- App Server
- EDI Server

**Central Services**
- Confidential Data

**MARKETING SUBNET**
- Marketing Users
- Marketing User 1 - Policies

**FINANCE SUBNET**
- Finance Users
- Finance User Group
- Marketing User 1 - Policies

**Access Control Lists**
- Marketing User 1 - Policies
  - Allow access to sales server
  - Allow remote access
  - Allow access to web server
  - Deny access to finance server
  - Deny access to confidential data

**Security Gateway Network Deployment Modes**

Freescale, the Freescale logo, AltVec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, mobileGT, PowerQUICC, StarCore, and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. BeeKit, BeeStack, CoreNet, the Energy Efficient Solutions logo, Flexis, MXC, Platform in a Package, Processor Expert, QorIQ, QUICC Engine, SMARTMOS, TurboLink and VortiQa are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2010 Freescale Semiconductor, Inc.
Security Zones Concept and Firewall Methodology

Firewall Types:
- Proxy
- Static packet filters
- Stateful inspection

Internet
{WAN}  P2020RDB + VortiQa  LAN

External Zone  The Self Zone  Corp Zone
Firewall Types

► Proxy Server Firewall

- Work at transport or application Layer
- No direct connection between internal server and external user
- Validate information based on access rules at service or application-specific level to provide best protection for applications
- Less flexible, slow and need more resources
Firewall Types (cont.)

► Static Packet Filtering Firewall
  • Operate at networking layer
  • Simple, but have limited protection and utility

► Static Packet Filtering Firewall
  • The state of the connection is monitored all the time
  • Filtering at network layer; screening up to application layer
  • Can dynamically change rules

Traffic filtering is based on the IP address, Packet type, Port number of the remote computer. Etc.

A typical firewall should filter at all the three levels of the TCP/IP Stack.
Firewall Packet Inspection Domain

IP selectors (source, destination addresses)

Transport protocol type and port selectors

Transport protocol state tracking

Firewall Packet Processing

| IP | TCP/UDP | Payload |
What Should Be Inspected During a Given DPI?
Deep Packet Inspection (DPI) Domain

- Inspect IP Header
- Inspect Transport Header
- Inspect Protocol Header
- Inspect Protocol Content (Payload)

TCP Buffering / re-sequencing

IPS Packet Processing

http header
http payload

http payload

http payload

http payload

http payload
DPI Operators?

► Malicious content tracking
  • Search packets for known malicious patterns

► Protocol state tracking
  • Validate application protocol parameters against known weaknesses and vulnerabilities
  • Allow only valid state transitions

► Traffic rates tracking
  • Enforce network utilization policies:
    ▪ Concurrent session counts
    ▪ Session setup rate
    ▪ Packet, bit or byte rate
Patterns, Regular Expression and “Regex” Formalism

- Formal language theory calls “patterns” regular expression or “Regex”

- Regex has many equivalent presentations

1. Perl Compatible Regular Expressions (PCRE)
   Performance issues

2. Deterministic Finite Automaton (DFA)
   State explosion issues

3. Nondeterministic Finite Automaton (NFA)
   Finite number of patterns can be supported.
DPI Implementation Options:

**Brute force DPI:** Apply all rules on all traffic type
- Simple system architecture
- Too many false positive
- Low system performance

**Classified DPI:** Divide rules into classes and apply only to relevant traffic
- Complex system architecture
- Lower false positive
- Higher performance

- **http rules**
  - http traffic
  - TCP traffic

- **FTP Rules**
  - FTP traffic
  - TCP traffic

- **UDP Rules**
  - UDP traffic
  - IP Traffic
DPI Deployment Scenarios:
Intrusion Detection System (IDS) vs. Intrusion Prevention System (IPS)
DPI Deployment Topology: IPS vs. IDS Deployment

DPI as an IDS “Tap mode”

- Traffic is sniffed only

IDS Manager

External Network

DPI as Inline IPS

- Traffic inspected inline

IPS Manager

Internal Networks

Inline L3 mode

• Packets are intercepted at the IP Layer.

Inline L2 mode

• Packet are intercepted at the bridge layer.
SOHO / Residential Gateway Deployment

- Malicious Hackers
- URL Keyword Filtering
- IPsec VPN
- Unauthorized Users
- Wireless Security
- Firewall
- OFFICE VPN CONNECTION
- Confidential Data
- Email Server
- EDI Server
- Laptop with Wireless LAN Connection 802.11A/G/N
- FRIENDS ONLINE
- SCHOOL WORK
- INTERNET
- BANKING SHOPPING NEWS AND ENTERTAINMENT TRAVEL AND LEISURE
- HOMEOFFICE
- HOMEEXTRA
- UNIVERSITY
Enterprise Network Equipment Deployment

Malicious Hackers
- Trojan Attack
- DoS Attacks
- Application Attacks
- OS Finger Printing Attacks
- Anti-NIDS Attacks

Internet

Enterprise Network
- Logging Console
- Admin Console
- DoS
- Web Server
- Confidential Data
- Corporate LAN
- Insider Attacks
- Un-patched Application security hole

DMZ
- Other Internal Users
- CENTRAL SERVICES
- Email Server
- App Server
- EDI Server

Marketing Subnet
- Marketing Users
- Finance Users

Finance Subnet
- Finance Users

Marketing Subnet
- Marketing Users

Other Internal Users

Confidential Data

Central Services

Web Server

Insider Attacks
DPI with VortiQa Software
DPI with VortiQa Software for Enterprise Network: Inline IPS

- Detects and prevents intrusions
  - Signature based detection
  - Protocol anomaly detection
  - Traffic anomaly detection

- Flexible to adopt various acceleration methods
  - Built-in software pattern-matching engines (software DFA engine, PCRE)
  - Fully integrated with PME 1.0 and PME 2.0

- P2P traffic detection, and traffic rate enforcement
  - Enforce concurrent session count settings
  - Enforce sessions rate settings

- Lower false positives
  - Context based signature verification
  - Application engines (HTTP, SMTP, FTP, TCP, UDP, IP)
  - Superior rule formats with application specific keywords
  - Rules classified to granular levels by application category
IPS rules are classified into various buckets to minimize search space.

- Rules are classified based on Application type.
- Rules are further divided into Content-Search Rules, Non-Content Rules. (Rules with header fields, flags, integers, etc)
VortiQa Software for Enterprise Network: Protocol Anomaly Detection

► Built-in traffic normalization – full defrag, reassembly and legal behavior enforcement
  • IP fragmentation overlap, options etc.
  • TCP segmentation overlap, options usage etc.
  • All checksum/length consistency

► Application protocol behavior – deep application protocol parsing
  • Illegal field values and combinations, e.g. DNS request
  • Illegal commands usage, e.g. HTTP and SMTP
  • Unusually long or short field lengths
  • Unusual number of occurrence of particular fields/commands
  • Unexpected state transition sequences – suggesting service configuration vulnerability or attack attempts
Sample of Protocol Anomaly Rules

- **18099**  SNMP: wrong data type
- **14999**  POP(3) Request Command Buffer Overflow Vulnerability
- **6099**  FTPd buffer overflow vulnerability
- **2999**  Smtp Data has more than maximum configured number of Boundaries.
- **349**  HTTP v0.9 Syntax Request detection
- **18098**  SNMP: wrong length
- **6098**  FTP Bounce Attack
- **2998**  Smtp Mime Header exceeding configured maximum limit
- **348**  IDS evasion detection - NULL Character at the end of URI
- **18097**  SNMP: wrong Version value
- **6097**  Invalid PORT command in FTP command line
- **2997**  Smtp Header Length exceeding configured maximum limit.
- **447**  HTTP multiple content length field vulnerability
- **347**  HTTP malformed Request detection
- **18096**  SNMP: wrong PDU value
- **6096**  Invalid FTP Command
- **2996**  SMTP command with command length exceeding 512 bytes detected.
- **446**  IIS %u Unicode wide character encoding vulnerability
- **346**  Detection of large number of request header lines
- **445**  Double Percent Hex encoding vulnerability
VortiQa Software for Enterprise Network: Traffic Anomaly Detection

► Administrators can define normal traffic behavior
  • Connection rates
  • Concurrent connection counts
  • Packet rates
  • Byte rates

► Anything exceeds normal behavior, is an anomaly
  • Limit traffic to configured rate
  • Block traffic for specified time period
VortiQa Software for Enterprise Network: Log Viewer and Reporting Facilities

- Logs and reports
  - List all real-time events for easy monitoring and administration
  - Examine and analyze event and conduct network forensic activities
  - Generate periodic reports
  - Generate alerts
### VortiQa Softeware IPS Signatures – Syntax and Semantics

**LOCAL** = rule:3011; pktdir:inbound; logth:1; 

timeth:5; issuemask:MMMMM; **SELECTOR** = SIP:202.16.10.1; 
DIP:172.16.3.5; IPPROTO:UDP; SP:666; DP:2140; DIR:INIT; **DETECT** = content: f-cmd.exe; **ACTION** = **TYPE**: info;

<table>
<thead>
<tr>
<th>Rule: 3011</th>
<th>Intoto rule Id, which has to be unique</th>
</tr>
</thead>
<tbody>
<tr>
<td>pktdir: inbound</td>
<td>Packet Direction.</td>
</tr>
<tr>
<td>logth:1</td>
<td>Log threshold value.</td>
</tr>
<tr>
<td>timeth:5</td>
<td>Time threshold value.</td>
</tr>
<tr>
<td>issuemask:MMMMM</td>
<td>Issue mask is used for the forensic record based threshold calculation for generating the log message.</td>
</tr>
<tr>
<td>SIP: 202.16.10.1</td>
<td>Source IP Address from which the packet is originating</td>
</tr>
<tr>
<td>DIP: 172.16.3.5</td>
<td>Destination IP Address</td>
</tr>
<tr>
<td>IPPROTO: UDP</td>
<td>Layer 4 protocol</td>
</tr>
<tr>
<td>SP: 666</td>
<td>Source port</td>
</tr>
<tr>
<td>DP: 2140</td>
<td>Destination port</td>
</tr>
<tr>
<td>DIR:INIT</td>
<td>Initiator</td>
</tr>
<tr>
<td>Content:f-cmd.exe</td>
<td>Contents to be detected in the packet</td>
</tr>
<tr>
<td><strong>TYPE</strong>: info</td>
<td>Generate log message</td>
</tr>
</tbody>
</table>
GUI based signature editor

- Enable user to author and upload locally created signatures on the fly
VortiQa Signature Server Infrastructures

► VortiQa signature servers offer periodic and manual signature download support

![Diagram showing VortiQa Signature Server Infrastructures]
Freescale Solution-Centric Approach Offers DPI Turnkey Solution
Continues Our Embedded Leadership Tradition

A new era of networking requires a new way of thinking.

Our Heritage:

► 3rd Generation Data Path
  • Gen-1: CPM MPC8260
  • Gen-2: QUICC Engine MPC8360
  • Gen-3: DPAA QorIQ P4080

► Accelerating Connectivity
  • eTSEC
  • SEC 4.0
  • PME 2.0
  • PCIe, Serial RapidIO, XAUI

► Power Architecture ISA
  • e500 PowerQUICC III
  • e500 QorIQ P1, P2 platforms
  • e500mc QorIQ P3, P4 platforms

Communications Processors

No. 1 supplier of communications processors  No. 1 in embedded for communications
## Deep Packet Inspection Performance Dependency Matrix

<table>
<thead>
<tr>
<th>Hardware capabilities Requirements vs UTM performance benefit cross reference matrix.</th>
<th>UTM Hardware</th>
<th>Firewall Forwarding</th>
<th>IPSec VPN throughput</th>
<th>IPS inspection</th>
<th>Anti-x inspections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet forwarding capability</td>
<td></td>
<td>IO throughput</td>
<td>IO throughput</td>
<td>IO throughput</td>
<td>IO throughput</td>
</tr>
<tr>
<td>IPSec offload</td>
<td></td>
<td></td>
<td>VPN Crypto performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pattern Matching offload</td>
<td></td>
<td></td>
<td>hardware assisted signature scanners</td>
<td>hardware assisted signature scanners</td>
<td></td>
</tr>
<tr>
<td>Processor Cache</td>
<td></td>
<td></td>
<td>Software signature scanners</td>
<td>Software signature scanners</td>
<td></td>
</tr>
<tr>
<td>Higher CPU clock capability</td>
<td></td>
<td></td>
<td>Software signature scanners</td>
<td>Software signature scanners</td>
<td></td>
</tr>
</tbody>
</table>

Firewall VPN Gateway

IPS and Anti Virus gateways
Freescale Recommended DPI Processors

In general, any Freescale processor could run DPI type application. However, the following processor families are expected to perform well.

► P1 and P2 P2020, P1020, P1011
  • L2 Cache
  • High CPU clock
  • Single / dual cores

► MPC8572
  • PME 1.1
  • L2 Cache
  • High CPU clock
  • Dual cores

► P4080
  • PME 1.1
  • DPAA architecture
  • L2 Cache
  • High CPU clock
  • Eight cores
Freescale Pattern Matching Engine Key Features

► MPC8572 PME 1.x

- The MPC8572 PowerQUICC III processor has an inbuilt pattern-matching engine (PME) that implements a NFA data examination engine with the following capabilities:
  - Up to 16000 Regex patterns can be configured and the patterns can be divided into 256 non-overlapping sets
  - Each set can have up to 16 subsets resulting in 256*16 groups
  - Pattern matching across packet boundaries
  - A max of 128M sessions are supported (with session context size of 32 bytes)
  - Stateful rule engine to enable application protocol tracking and stateful pattern matching
  - Pattern lengths between 1 and 128 bytes
  - A max of 8192 stateful rules are supported

► P4080 PME 2.x

- The P4080 QorIQ processor has a built-in pattern-matching engine that implements a NFA data examination engine with the following capabilities:
  - 32000 Regex patterns can be configured and the patterns can be divided into 256 non-overlapping sets
  - Each set can have up to 16 subsets resulting in 256*16 groups
  - Pattern matching across packet boundaries
  - Stateful rule engine to enable application protocol tracking and stateful pattern matching
  - Pattern lengths between 1 and 128 bytes
Freescale VortiQa software products are designed to accelerate product development and increase the pace of innovation.

Market segment focus:
- IP services
- Security appliances
- SMB and multi-service business gateways (MSBGs)

VortiQa product lines of production-ready software applications:
- VortiQa software for service provider equipment
- VortiQa software for enterprise network equipment
- VortiQa software for small business gateways
- VortiQa software for SOHO/residential gateways

A comprehensive solution-centric approach for networking applications in targeted vertical segments:
- Silicon – QorIQ and PowerQUICC communications processors
- Software – VortiQa software products
- Expanded ecosystem - hardware, OS, ISVs and system integrators
## Freescale UTM Appliance Performance

*Highly Competitive Performance*

<table>
<thead>
<tr>
<th>UTM Appliance</th>
<th>Firewall</th>
<th>IPsec VPN AES32-SHA1</th>
<th>IPsec VPN 3DES-SHA1</th>
<th>IPS SW DFA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UTM-2020, 1.2 GHz, 2 cores</strong></td>
<td>4 Gbps</td>
<td>1.3 Gbps</td>
<td>1.3 Gbps</td>
<td>494 Mbps</td>
</tr>
<tr>
<td>VortiQa software for enterprise equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UTM-4080, 1.5 GHz, 8 cores</strong></td>
<td>20 Gbps*</td>
<td>10 Gbps*</td>
<td>10 Gbps*</td>
<td>N/A</td>
</tr>
<tr>
<td>VortiQa software service provider equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UTM-8572, 1.5 GHz, 2 cores</strong></td>
<td>4 Gbps</td>
<td>1.4 Gbps</td>
<td>1.3 Gbps</td>
<td>661 Mbps</td>
</tr>
<tr>
<td>VortiQa software for enterprise equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Performance numbers are measured or estimated for big packet size traffic
- Firewall performance is saturated at line rate
- P4080-based UTM performance estimates based on cycle-accurate model
Test Objective:
Show VortiQa Linux SMP / firewall P2020 performance capabilities

Required data:
1. Live data: UDP traffic, for 64, IMIX, and 512 bytes packets.
VortiQa Security Appliance
Firewall Performance

Secure Appliance P2020 1.0Ghz - VortiQa Firewall

Performance measurement configuration footnotes:

Silicon: P2020
Per Core CPU frequency: 1.0 Ghz
L1-I/L1-D/L2/L3 Cache: TBD

Board: Security Appliance
DDR Frequency: 1.3 Ghz
RAM: 4 GB

Board Clock: TBD Mhz
Sec 4 Frequency: TBD Mhz
Interfaces: 4 x 1 GbE;
Test Objective:
Show VortiQa enterprise IPS capabilities using Breaking Point tools

Required data:
1. http server side attacks coverage
2. Others …
VortiQa Security Appliance
IPS (with Firewall) Performance

Security Appliance P2020 1.0Ghz IPS Performance

Performance measurement configuration footnotes:

Silicon: P2020
Per Core CPU frequency: 1.0 Ghz
L1-I/L1-D/L2/L3 Cache: TBD

Board: Security Appliance
DDR Frequency: 800 Mhz
RAM: 4 GB

Board Clock: TBD Mhz
Sec 3 Frequency: TBD Mhz
Interfaces: 4 x 1 GbE;
VortiQa Software for Service Provider
P4080 10 Gbps Firewall Performance - DPAA

- Dell XAUI 10G BaseT Interface {Rear}
  - Aggregate 10 1G interfaces into 1 10G interface
- Dell 10 1 G BaseT Interface {Front}
- IXIA 10 1 G BaseT Interface
- VLAN 1, VLAN 2, VLAN 3, VLAN 4, VLAN 5, VLAN 6, VLAN 7, VLAN 8, VLAN 9, VLAN 10

IXIA
VortiQa Application Performance

Line Rates

P4080 VortiQa NAT+Firewall Application Performance
(Using 1 XAUI Interface)

Performance measurement configuration footnotes:

Silicon: P4080 Rev1
Per Core CPU frequency: 1.5 Ghz
L1-I/L1-D/L2/L3 Cache: 32K/32K/128K/2MB
Firewall: 1 K Sessions

Board: Rev B  P4080 DS
DDR Frequency: 1.3 Ghz
RAM: 4 GB
IPSec: 8 Tunnels

Board Clock: 700 Mhz
Sec 4 Frequency: 350 Mhz
Interfaces: 1 x 10 GbE;
VortiQa Application Performance
Substantial Processor Headroom

P4080 VortiQa NAT+Firewal CPU Utilization at Optimal Performance
(Using 1 XAUI Interface)

Performance measurement configuration footnotes:

Silicon: P4080 Rev1
Per Core CPU frequency: 1.5 Ghz
L1-L1-D/L2/L3 Cache: 32K/32K/128K/2MB
Firewall: 1 K Sessions

Board: Rev B  P4080 DS
DDR Frequency: 1.3 Ghz
RAM: 4 GB
Sec 4 Frequency: 350 Mhz
Interfaces: 1 x 10 GbE;

IPSec: 8 Tunnels
VortiQa Application Performance
20 Gbps

P4080 VortiQa Firewall Application Performance
(Projected with 2XAUI Interfaces)

Performance measurement configuration footnotes:

Silicon: P4080 Rev1
Per Core CPU frequency: 1.5 Ghz
L1-I/L1-D/L2/L3 Cache: 32K/32K/128K/2MB
Firewall: 1 K Sessions

Board: Rev B P4080 DS
DDR Frequency: 1.3 Ghz
RAM: 4 GB
IPSec: 8 Tunnels

Board Clock: 700 Mhz
Sec 4 Frequency: 350 Mhz
Interfaces: 1 x 10 GbE;
Security Appliance Segment Mapping
High-level Overview

**Datacenter/Carrier**
- FW throughput: 6 – 10 Gbps
- VPN tunnels: 100K
- FW/IPS sessions: 1 Million
- FW policies: 10K; sessions/s:100K
- VPN: 5-10Gbps; Tunnels/sec: 500
- Firewall/IPS: 4-8 Gbps
- Anti Virus: 2500 HTTP obj./sec

**Mid-/High-end Enterprise**
- FW throughput: 2-5 Gbps
- VPN tunnels: 10K
- FW/IPS sessions: 250K
- FW policies: 5K; sessions/s:15K
- VPN: 1-2 Gbps; Tunnels/sec: 50
- Firewall/IPS: 1-2 Gbps
- Anti Virus: 500 HTTP obj./sec

**Small Enterprise/SME**
- FW Throughput: 1-2 Gbps
- VPN tunnels: 2K
- FW/IPS sessions: 100K
- FW policies: 1k; sessions/s:5K
- VPN: 500Mbps; Tunnels/sec: 10
- Firewall/IPS: 500Mbps – 1Gbps
- Anti Virus: 100 HTTP obj./sec

**Small Business**

Notes on Performance / Cost Estimates:
- Subject to hardware configuration; may vary substantially
- All performance numbers are target numbers as estimated to be required for individual deployments and are estimated with VortiQa software product; subject to interpretation and detailed analysis

PowerQUICC MPC83xxE processor family
- QorIQ P1 and P2 processor family
- OS and BSP – Linux®
- VortiQa software for enterprise equipment

PowerQUICC MPC85xxE processor family
- QorIQ P4, P5 processor family
- OS and BSP – Linux and/or LWE
- VortiQa software for service provider equipment
## UTM Security Appliance Solutions - Portfolio

<table>
<thead>
<tr>
<th>UTM Appliance</th>
<th>ODM</th>
<th>Freescale Processor</th>
<th>Cores</th>
<th>Core Frequency</th>
<th>Schedule</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTM-2010</td>
<td>Portwell</td>
<td>QorIQ P2010E</td>
<td>1</td>
<td>1 GHz</td>
<td>August 2010</td>
<td>Small enterprise value systems; highest performance with lower power in its class</td>
</tr>
<tr>
<td>UTM-2020</td>
<td>Portwell</td>
<td>QorIQ P2020E</td>
<td>2</td>
<td>1 GHz/1.2 GHz</td>
<td>August 2010</td>
<td>Mid enterprise, low power systems</td>
</tr>
<tr>
<td>UTM-4080</td>
<td>Advantech and O2 Security</td>
<td>QorIQ P4080E</td>
<td>8</td>
<td>1.5 GHz</td>
<td>TBD</td>
<td>High-end enterprise or service provider systems</td>
</tr>
<tr>
<td>UTM-8572</td>
<td>O2 Security</td>
<td>MPC8572E PowerQUICC III</td>
<td>2</td>
<td>1.2 GHz</td>
<td>Now</td>
<td>Mid-enterprise IPS based deployments</td>
</tr>
<tr>
<td>UTM-8540</td>
<td>O2 Security</td>
<td>MPC8540 PowerQUICC III</td>
<td>1</td>
<td>667 MHz/1 GHz</td>
<td>Now</td>
<td>Small to mid enterprise</td>
</tr>
</tbody>
</table>

- ODM sample boxes are available now
- Schematics and Gerber files are available for Freescale prototype of UTM-2020