FORCEPOINT

Next Generation Firewall

Release Notes

6.4.2

Revision B

Contents

About this release

This document contains important information about this release of Forcepoint Next Generation Firewall (Forcepoint NGFW).

We strongly recommend that you read the entire document.

Lifecycle model

This release of Forcepoint NGFW is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Forcepoint NGFW is available.

We recommend using the most recent Long-Term Support (LTS) version if you do not need any features from a Feature Stream version.

For more information about the Forcepoint NGFW lifecycle policy, see Knowledge Base article 10192.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

Forcepoint NGFW appliances

We strongly recommend using a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations.

Note: Some features in this release are not available for all appliance models. See Knowledge Base article 9743 for up-to-date appliance-specific software compatibility information.

The following table shows whether you can use an appliance model in the Firewall/VPN (FW), IPS, or Layer 2 Firewall (L2FW) role.

Appliance model	Roles
320X (MIL-320)	FW
FWL321	FW
NGF321	FW, IPS, L2FW
FWL325	FW
NGF325	FW, IPS, L2FW
110	FW
115	FW
330	FW, IPS, L2FW
331	FW, IPS, L2FW
335	FW, IPS, L2FW
1035	FW, IPS, L2FW
1065	FW, IPS, L2FW
1101	FW, IPS, L2FW
1105	FW, IPS, L2FW
1401	FW, IPS, L2FW
1402	FW, IPS, L2FW
2101	FW, IPS, L2FW
2105	FW, IPS, L2FW
3202	FW, IPS, L2FW
3206	FW, IPS, L2FW
3207	FW, IPS, L2FW
3301	FW, IPS, L2FW

Appliance model	Roles
3305	FW, IPS, L2FW
5206	FW, IPS, L2FW
6205	FW, IPS, L2FW

Sidewinder S-series appliances

These Sidewinder appliance models can be re-imaged to run Forcepoint NGFW software.

Appliance model	Roles
S-1104	FW
S-2008	FW
S-3008	FW
S-4016	FW
S-5032	FW
S-6032	FW

Certified Intel platforms

We have certified specific Intel-based platforms for Forcepoint NGFW.

The tested platforms can be found at https://support.forcepoint.com under the Forcepoint Next Generation Firewall product.

We strongly recommend using certified hardware or a pre-installed Forcepoint NGFW appliance as the hardware solution for new Forcepoint NGFW installations. If it is not possible to use a certified platform, Forcepoint NGFW can also run on standard Intel-based hardware that fulfills the hardware requirements.

Basic hardware requirements

You can install Forcepoint NGFW on standard hardware with these basic requirements.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher

  Note: Legacy deployments with Intel® Core™2 are supported.

- IDE hard disk and DVD drive

  Note: IDE RAID controllers are not supported.

- 4 GB RAM minimum
- VGA-compatible display and keyboard
- One or more certified network interfaces for the Firewall/VPN role
- Two or more certified network interfaces for IPS with IDS configuration

- Three or more certified network interfaces for Inline IPS or Layer 2 Firewall

For information about certified network interfaces, see Knowledge Base article 9721.

Master NGFW Engine requirements

Master NGFW Engines have specific hardware requirements.

- Each Master NGFW Engine must run on a separate physical device. For more details, see the *Forcepoint Next Generation Firewall Installation Guide*.
- All Virtual NGFW Engines hosted by a Master NGFW Engine or Master NGFW Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master NGFW Engines can allocate VLANs or interfaces to Virtual NGFW Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Firewalls is *Normal* (fail-close) and you want to allocate VLANs to several engines, you must use the Master NGFW Engine cluster in standby mode.
- Cabling requirements for Master NGFW Engine clusters that host Virtual IPS engines or Layer 2 Firewalls:
  - Failure Mode *Bypass* (fail-open) requires IPS serial cluster cabling.
  - Failure Mode *Normal* (fail-close) requires Layer 2 Firewall cluster cabling.

  For more information about cabling, see the *Forcepoint Next Generation Firewall Installation Guide*.

Virtual appliance node requirements

You can install Forcepoint NGFW on virtual appliances with these hardware requirements. Also be aware of some limitations.

- (Recommended for new deployments) Intel® Xeon®-based hardware from the E5-16xx product family or higher

  Note: Legacy deployments with Intel® Core™2 are supported.

- One of the following hypervisors:
  - VMware ESXi 6.0 and 6.5
  - KVM (KVM is tested as shipped with Red Hat Enterprise Linux Server 7.1 and 7.2)
  - Microsoft Hyper-V on Windows Server 2012 or Windows Server 2016 (Firewall/VPN role only)
    An Intel 64-bit processor is required.
- 8 GB virtual disk
- 4 GB RAM minimum
- A minimum of one virtual network interface for the Firewall/VPN role, three for IPS or Layer 2 Firewall roles
  The following network interface card drivers are recommended:
  - VMware ESXi platform — `vmxnet3`.
  - KVM platform — `virtio_net`.

When Forcepoint NGFW is run as a virtual appliance node in the Firewall/VPN role, these limitations apply:

- Only Packet Dispatching CVI mode is supported.
- Only standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

When Forcepoint NGFW is run as a virtual appliance node in the IPS or Layer 2 Firewall role, clustering is not supported.

Supported cloud environments

You can deploy Forcepoint NGFW in the Amazon Web Services (AWS) and Microsoft Azure cloud environments.

Amazon Web Services

Forcepoint NGFW instances can be launched from AWS using 1-Click Launch, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available instance types, search for *Forcepoint NGFW* in the AWS Marketplace.

For more information about deploying in AWS, see the document *How to deploy Next Generation Firewall in the Amazon Web Services cloud* and Knowledge Base article 10156.

Microsoft Azure

Forcepoint NGFW instances can be launched from Azure using custom solution templates, and existing instances can be remotely upgraded to the latest Forcepoint NGFW version.

To see the currently available custom solution templates, search for *Forcepoint NGFW* in the Azure Marketplace.

For more information about deploying in Azure, see the document *How to deploy Next Generation Firewall in the Azure cloud* and Knowledge Base article 14485.

Build version

Forcepoint NGFW 6.4.2 build version is 20106.

Product binary checksums

Use the checksums to make sure that the installation files downloaded correctly.

- sg_engine_6.4.2.20106_x86-64-small.iso

```
SHA1SUM:
d482843141b55f0dfc4d9d2b80dbd413da15d787

SHA256SUM:
5fedd281d14a803db18ab1fbceb11b4774f032aa4fb5ffb519f8beb0ea31c202

SHA512SUM:
82892a15445fd0896e581d507a4f3030
4091f64c30fb78f2ce5584c75c5bc646
554bc85bb415e27cd24d0d45d027d03e
4b2be8ca84bc3f1a4b99cb9272f54c26
```

- sg_engine_6.4.2.20106_x86-64-small.zip

```
SHA1SUM:
ee9d9ef0faebac9db7f58a304701f448d79689eb

SHA256SUM:
9361f6910e4640b24b67314d9073937a6710d0cadf8c9712809447976d60abbc

SHA512SUM:
a4c8f9faa469aba70453947d5fe6d015
53c252701df553c1696717f38ad021ea
c5a592b7dafa0310a9e0380854611130
c1d15a2ccc94396f6375d9a64f28ac1d
```

Compatibility

Forcepoint NGFW 6.4 is compatible with the following component versions.

- Forcepoint NGFW Security Management Center (SMC) 6.4 or higher
- Dynamic Update 1041 or higher
- Stonesoft® VPN Client for Windows 6.0.0 or higher
- Stonesoft® VPN Client for Mac OS X 2.0.0 or higher
- Stonesoft® VPN Client for Android 2.0.0 or higher
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) 1.1.0 or higher
- Forcepoint User ID Service 1.1.0 or higher
- McAfee® Logon Collector 2.2 and 3.0

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

Redirection of HTTP and HTTPS traffic to a proxy

The NGFW Engine can now transparently redirect HTTP and HTTPS traffic to a proxy. The proxy can be on-premises or a cloud-based service, such as the Forcepoint Web Security Cloud service. The traffic does not have to be redirected through a policy-based VPN.

Improved integration of external NTP servers

You can now use external NTP servers to provide time synchronization for both the SMC Appliance and NGFW Engines. External NTP servers were previously supported only for the SMC Appliance. You can use the same NTP servers for the SMC Appliance and the NGFW Engines.

SNMP Agent enhancements

You can now use SNMP Agents when you configure SNMP for the SMC Appliance. SNMP Agents were already supported for NGFW Engines in previous versions.

You can now specify the SNMP engine ID for each NGFW Engine and for the SMC Appliance. The SNMP engine ID is a unique identifier that the SNMP Agent uses to for the NGFW Engine or the SMC Appliance.

SNMP Agents now support IPv6 addresses.

Note: If you configured SNMP for the SMC Appliance before upgrading to version 6.4, you must configure SNMP again after upgrading to version 6.4.0 or higher.

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint NGFW version 6.4.0

Enhancement	Description
Improved integration of external LDAP servers and Active Directory servers	The integration of external LDAP servers and Active Directory servers with Forcepoint NGFW has been improved. • Support for the LDAPS and Start TLS protocols for securing the LDAP connection has been improved. When LDAPS or Start TLS is enabled for an LDAP Server or Active Directory Server, you can now select a TLS Profile and TLS Server Identity for the LDAP Server. • A new Authentication Method element for LDAP Authentication has been added. When LDAP Authentication is configured for a user, the user's password is checked against the user's credentials in the LDAP server that is used for user storage. LDAP Authentication can be used with the following existing features: IPsec and SSL tunnels in mobile VPNs, the SSL VPN Portal, and browser-based user authentication.
Improvements in browser-based user authentication	Browser-based user authentication now supports certificate-based authentication. Users can authenticate using a certificate file, or a certificate stored on a smart card, such as a Common Access Card (CAC).
Other authentication enhancements	The **Require Authorization** and **Timeout for Client IP Authorization** options have been removed from Authentication options for Access rules. Authorization is automatically required when you add User and Authentication Method elements to the **Authentication** cell. The **Authentication Time-Out** option in the **Add-Ons** > **User Authentication** branch of the Engine Editor replaces the **Timeout for Client IP Authorization** option.

Enhancement	Description
Improvements in application detection	Because Access rules for application detection match traffic based on the payload of connections, the same connection can potentially match more than one rule based on the first SYN packet of the connection. Connection handling such as the use of VPNs, NAT, SSM Proxies, and TCP MSS enforcement is applied according to the initial match. When the final match is different from the initial match in a way that changes connection handling, the connection is dropped. In these cases, a log message that indicates a conflict between rules is generated. **Note:** Due to changes in application detection, policies that use Network Applications, URL Categories, or URL Lists in the Access rules might work differently after upgrading to NGFW 6.4. Some traffic that was previously allowed might be discarded. After upgrading to NGFW 6.4 or higher, verify that your policies work as expected. For more information, see Knowledge Base article 15411.
New Network Application elements of the Cloud Services type	New Network Application elements of the Cloud Services type have been added to the SMC from the Forcepoint cloud access security broker (CASB) service catalog. Including the previous Network Application elements of the Web Applications and Protocols types, there are now over 7000 Network Applications available.
Duplicate IPv6 address detection for Layer 3 Physical Interfaces	An option for detecting duplicate IPv6 addresses has been added to the Layer 3 Physical Interface properties for NGFW Engines.
Bootloader password for NGFW Engines	During the initial configuration, you can now specify a bootloader password for the NGFW Engine. To edit the options that appear in the bootloader, you must enter the bootloader password.
Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls	You can now configure Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls.
Easier deployment of NGFW Engines in Microsoft Azure	You can now deploy NGFW Engines from the Microsoft Azure cloud environment without first creating the NGFW Engine element in the Management Client. You deploy the NGFW Engines from the cloud environment, and you can monitor the NGFW Engines in the Management Client.
Auto-scaling in Microsoft Azure	Support for auto-scaling for NGFW Engines that are deployed in Azure has been added. When the scaling feature is used, additional NGFW Engine instances are automatically created and removed, depending on traffic load. You can monitor the NGFW Engine instances in the Management Client.
Cloud Sandbox analysis information in the external portal	You can now view analysis information in the external portal for the cloud sandbox. You must define a user name for the cloud service in the Management Client to be able to view the analysis information in the external portal.
Auto-discovery for ECA clients	The NGFW Engine can now advertise its contact address to ECA clients. If the contact address of the NGFW Engine changes, or a new NGFW Engine is added to the network, the ECA clients are still able to connect to the NGFW Engine.
Monitoring of Forcepoint User ID Service	You can now enable monitoring for the Forcepoint User ID Service. You can also configure that the Forcepoint User ID Service sends log data to the SMC.
License reporting tool	There is a new tool for MSSP customers that exports all data related to licenses and NGFW Engines to a CSV file.

Enhancements in Forcepoint NGFW version 6.4.1

Enhancement	Description
QoS throughput alerts added	An alert is now triggered when the QoS throughput limit defined for a Virtual Security Engine is exceeded.

Enhancements in Forcepoint NGFW version 6.4.2

Enhancement	Description
Additional cipher support added	Client and server protection features now support additional ciphers.
Session-Duplicate-Mac situation element	The Session-Duplicate-Mac situation is logged when a different VPN Client user connects using the same MAC address as a VPN Client that is already connected, replacing the previous user.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Role	Issue number
When a VPN endpoint that has a dynamic IP address uses a fully qualified domain name (FQDN) as the contact address, Multi-Link VPNs do not work correctly. The firewall discards Multi-Link probe and status messages.	FW	NGFW-2298
When you add or remove an Aggregated Link interface, traffic that uses the Aggregated Link interfaces might be interrupted.	FW	NGFW-5031
When inspection is used on appliance models N110 and N115, policy upload might fail.	FW	NGFW-7973
Client or server protection might not work for connections which require using ECDH key exchange.	FW, IPS, L2FW	NGFW-9766
Connections to Microsoft services that are subject to client or server protection and file filtering might not work.	FW, IPS, L2FW	NGFW-10194
The ECA Computer Name column in the Logs view does not contain any information.	FW, IPS, L2FW	NGFW-10224
When IPsec VPNs are configured on an NGFW Engine, memory consumption can increase substantially. In extreme cases, all the available memory can be consumed, causing the NGFW Engine to become unstable.	FW	NGFW-10281
NGFW Engines that have PPP interfaces might restart, and kerneldump files might be created.	FW	NGFW-10552
NGFW Engines might not validate LDAPS server certificates according to the settings in the TLS profile.	FW, IPS, L2FW	NGFW-10603

Description	Role	Issue number
If the same AS number is prepended multiple times for a BGP Route Map in the SMC configuration, the AS number is prepended only once in the Route Map when checking it using vtysh.	FW	NGFW-10660
When a policy is installed or refreshed, dynamic routing processes might restart unnecessarily.	FW	NGFW-10661
When you take traffic captures using the Management Client, the Capture Traffic tool produces corrupted capture files.	FW, IPS, L2FW	NGFW-10735
When HTTPS connections are inspected, the connections might not be closed properly if URL filtering is used and TLS decryption is not used.	FW, IPS, L2FW	NGFW-10750
In a Firewall Cluster that includes some nodes running version 5.10 and some nodes running version 6.2 or higher, BGP routes are not synchronized to the nodes running version 5.10.	FW	NGFW-10806
The amount of memory used when a large number of Endpoint Context Agent (ECA) clients are connected can be excessive.	FW, IPS, L2FW	NGFW-10822
Firewall nodes continue to send gratuitous ARP requests for MAC addresses that received virtual IP addresses even after the clients have disconnected. If the same host connects to a network that is directly connected to the firewall and receives the same IP address from the DHCP server, a MAC address conflict is created.	FW	NGFW-10870
In Multi-Link VPNs, tunnels that use standby link mode might send connectivity probes even when they are not active.	FW	NGFW-10875
If the inspection process is using a large amount of memory when you install a policy, the Virtual NGFW Engine might fail to free the memory. The policy installation fails and the Master NGFW Engine node restarts.	FW, IPS, L2FW	NGFW-10888
Enabling both PIM multicast routing and OSPFv2 dynamic routing for the same interface removes the OSPFv2 authentication settings.	FW	NGFW-10893
When you use LDAP user authentication, some log entries might not include user information.	FW	NGFW-10915
The dmesg for the NGFW Engine might include the following message multiple times: "netlink: 12 bytes leftover after parsing attributes in process `smonitd'".	FW	NGFW-11067
When the User Monitoring view is open, the reception of new user information slows down.	FW, IPS, L2FW	NGFW-11175
When HTTPS connections are inspected, the inspection process might become unstable. As a result, latency increases for the inspected traffic.	FW, IPS, L2FW	NGFW-11190
The TLS_Incomplete-Configuration-For-Decrypting situation might be logged when TLS decryption is not configured or not allowed. By default, TLS decryption is allowed when you configure application detection or URL categorization.	FW, IPS, L2FW	NGFW-11233
Inspection of file downloads can become slow if the download arrives in smaller pieces, out of order. An example is Microsoft Windows update files.	FW, IPS, L2FW	NGFW-11261
The System Connections pane in the Home view shows always 0 connected Endpoint Clients for single NGFW Engine elements.	FW, IPS, L2FW	NGFW-11272
In rare situations, active FTP data connections can fail to open when inspection is used.	FW	NGFW-11319

Description	Role	Issue number
Inspection of a downloaded archive file that contains another archive file can severely slow down traffic processing.	FW, IPS, L2FW	NGFW-11320
When NGFW Engines cannot connect to the Log Server, the NGFW Engine might fail to send some log entries after the connection to the Log Server is re-established. If the Log Server to which the NGFW Engine sends logs changes, some log entries sent again to the new Log Server.	FW, IPS, L2FW	NGFW-11347
When deep inspection is enabled, the NGFW Engine might restart when you install a policy.	FW, IPS, L2FW	NGFW-11392
When Sidewinder Proxy is enabled, the SSM proxy process might restart.	FW	NGFW-11401
In Master NGFW Engine clusters, the node that is not involved in the IPsec SA renegotiation does not have the correct status for the SA after the renegotiation.	FW	NGFW-11471
When the node in a Firewall Cluster that is handling an active SIP connection changes, the new node might incorrectly modify the SIP payload.	FW	NGFW-11502
The SNMP MIB for link speed always reports the link speed as 0.	FW, IPS, L2FW	NGFW-11670
In rare cases when you use connection monitoring, the NGFW Engine might log a large number of "Connection Monitoring problem" messages from the monitoring facility.	FW, IPS, L2FW	NGFW-11709
When VPN gateways have endpoints with dynamic IP addresses, VPN logs might show the wrong gateway as the remote gateway.	FW	NGFW-11742
When traffic uses the HTTP (SafeSearch) service and there is a potentially matching rule before a rule that uses a Network Application in the Service cell, the inspection process might restart.	FW, IPS, L2FW	NGFW-11805
If IPsec SA renegotiation for a VPN fails, the existing IKE SA might be deleted.	FW	NGFW-11806
When an NGFW Engine node goes offline, it might send gratuitous ARP for automatic proxy ARP entries using the hardware MAC address of the node.	FW	NGFW-11847
In rare cases, FTP control connections might cause the inspection process to restart.	FW	NGFW-11919
Policy installation might take a long time if you use server pools and the defined DNS server is unreachable.	FW	NGFW-11964
When you use IPsec VPN tunnels with IPv6 endpoints, the NGFW Engine might restart.	FW	NGFW-11984
When you use route redistribution with dynamic routing, redistribution does not stop when a peer becomes unavailable if the same route is available from another routing daemon.	FW	NGFW-12078
In rare cases, the automatic certificate renewal might fail on the NGFW Engine, for example, after the Management Server certificate has been renewed.	FW, IPS, L2FW	NGFW-12111

Installation instructions

Use these high-level steps to install SMC and the Forcepoint NGFW engines.

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com.

> **Note:** The sgadmin user is reserved for SMC use on Linux, so it must not exist before SMC is installed for the first time.

> **Note:** If you install the SMC on Windows 10 and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.
2) Import the licenses for all components.

   You can generate licenses at https://stonesoftlicenses.forcepoint.com.
3) Configure the Firewall, IPS, or Layer 2 Firewall elements with the Management Client using the **Configuration** view.
4) To generate initial configurations for the engines, right-click each Firewall, IPS, or Layer 2 Firewall element, then select **Configuration** > **Save Initial Configuration**.

   Make a note of the one-time password.
5) Make the initial connection from the engines to the Management Server, then enter the one-time password.
6) Create and upload a policy on the engines using the Management Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, engines, and clusters.

> **Note:** Upgrading to version 6.4 is only supported from version 6.3 or higher. If you have a lower version, first upgrade to version 6.3.

> **Note:** Starting from Forcepoint NGFW version 6.4, the McAfee Advanced Threat Defense feature is no longer supported. We recommend that you use Forcepoint Advanced Malware Detection instead.

- Forcepoint NGFW version 6.4 requires an updated license. The license upgrade can be requested at https://stonesoftlicenses.forcepoint.com. Install the new license using the Management Client before upgrading the software. If communication between the SMC and the license server is enabled and the maintenance contract is valid, the license is updated automatically.

- To upgrade the engine, use the remote upgrade feature or reboot from the installation DVD and follow the instructions. For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.
- If you have customized the sshd_config file in the /data/config/ssh directory, you might need to manually update the configuration file after upgrading the engine to Forcepoint NGFW version 6.4. See Knowledge Base article 10461.

Known issues

For a list of known issues in this product release, see Knowledge Base article 15420.

Known limitations

This release of the product includes these known limitations.

Limitation	Description
Inspection in asymmetrically routed networks	In asymmetrically routed networks, using the stream-modifying features (TLS Inspection, URL filtering, and file filtering) can make connections stall.
Inline Interface disconnect mode in the IPS role	The *disconnect mode* for Inline Interfaces is not supported on IPS virtual appliances, IPS software installations, IPS appliance models other than IPS-6xxx, or modular appliance models that have bypass interface modules.

For information about feature-specific limitations, see the *Forcepoint Next Generation Firewall Product Guide*.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at https://support.forcepoint.com. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall online Help

> **Note:** By default, the online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

- *Forcepoint Next Generation Firewall Hardware Guide* for your model
- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API Reference Guide*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*